

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number  
**WO 02/25438 A1**

(51) International Patent Classification: **G06F 9/455**

(21) International Application Number: **PCT/US01/29863**

(22) International Filing Date:  
20 September 2001 (20.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/234,680 22 September 2000 (22.09.2000) US

(71) Applicant: **PATCHLINK.COM CORPORATION**  
[US/US]; Suite 123 PMB175, 3370 N. Hayden Rd.,  
Scottsdale, AZ 85251 (US).

(72) Inventors: **MOSHIR, Sean**; 3370 N. Hayden Rd. #123-  
175, Scottsdale, AZ 85251 (US). **ANDREW, Christopher**,

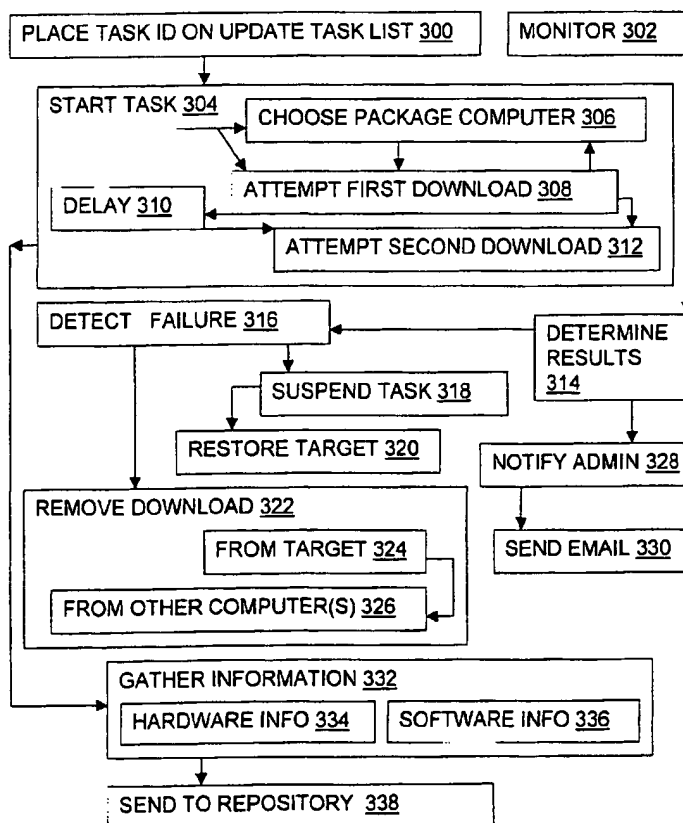
A., H.; 3290 West Mulberry Drive, Chandler, AZ 85248 (US). **HUDLER, Jack, Lee**; 619 Rainforest Lane, Allen, TX 75013 (US). **LI, Leon**; P.O. Box 41643, Mesa, AZ 85274 (US). **GORDON, Jonathan, M.**; 5001 East Hilton Ave, Mesa, AZ 85206 (US). **BACON, Michael**; 15850 N. Thompson Peak Pkwy #2051, Scottsdale, AZ 85260 (US). **WILLIAMS, Noah**; 9491 East Sandy Vista Drive, Scottsdale, AZ 85262 (US). **LANE, Jonathan**; 8687 Moss Creek Court, Reno, NV 89506 (US). **HORTON, James, J.**; 136 North Brett St., Gilbert, AZ 85234 (US). **FERGUSON, Dan**; 51 W. Center St. #247, Orem, UT 84057 (US).

(74) Agent: **OGILVIE, John, W., L.**; Computer Law++, 1211 East Yale Avenue, Salt Lake City, UT 84105 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,

[Continued on next page]

(54) Title: **NON-INVASIVE AUTOMATIC OFFSITE PATCH FINGERPRINTING AND UPDATING SYSTEM AND METHOD**



(57) Abstract: Methods, systems, and configured storage media including a discovery agent (548) are provided for discovering software updates, discovering if a given computer (202) can use the software update, and then updating the computers with the software as needed automatically across a network (200) without storing the updates on an intermediate machine within the network. Furthermore, when a failure (316) is detected, the rollout is stopped and the software can be automatically removed (324) from those computers that already were updated. The software update can be stored originally at an address that is inaccessible through the network firewall (214) by intermediately uploading the software update to an update computer (220) which is not a part of the network but has access through the firewall, which is then used to distribute the update.



MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL,  
TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

**Published:**

— with international search report

**(84) Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## **NON-INVASIVE AUTOMATIC OFFSITE PATCH FINGERPRINTING AND UPDATING SYSTEM AND METHOD**

### **RELATED APPLICATIONS**

5           This application claims priority to, and incorporates by reference, provisional U.S. patent application serial no. 60/234,680 filed September 22, 2000.

### **COPYRIGHT NOTICE**

          A portion of the disclosure of this patent document contains material which is  
10   subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. The copyright owner does not hereby waive any of its rights to have this patent document maintained in secrecy, including without limitation its rights pursuant to  
15   37 C.F.R. § 1.14.

### **FIELD OF THE INVENTION**

          The present invention relates to systems and methods which update existing software across a remote network. The invention relates more specifically to checking for  
20   the need for updating and then updating the software as required across a client-server system without the need for human oversight, and without requiring that a target network administrative machine keep copies of software patches.

### **TECHNICAL BACKGROUND OF THE INVENTION**

25           The 'state of the art' in the computer software industry remains such that software is often delivered with various anomalies in its desired behavior. These anomalous behaviors have come to be called "bugs".

          The original computer bug is in the operations log of the Harvard University Mark II Aiken Relay Calculator, now preserved in the Smithsonian. The operators removed a  
30   moth that had become trapped between relay switches in the computer, and wrote the entry "First actual case of bug being found." Problems with computer hardware and software have since been called "bugs", with the process of removing problems called "debugging".

Each time software is “debugged”, a change to that piece of software is created – this change sometimes results in an additional piece of software called a “patch” or “fix”. The industry’s software vendors often call these patches by the more formal names “Service Packs” or “Support Packs.”

5        This process has become so prevalent in the industry that software vendors use various naming and numbering schemes to keep track of their available “Support Packs”. The difficulty of keeping these “Support Packs” straight is increased when vendors fail to agree on a standard scheme of naming and numbering.

Microsoft, for instance, for its Windows NT family of operating system software  
10       products has no less than six major “Service Packs” available to be applied to solve problems its customers may experience. More generally, the total number of patches, fixes, solutions, and/or service packs for any given operating system may be enormous.

When an application is installed, it may contain one or more of these operating systems file patches along with the standard computer files. The patches are generally  
15       included because the application vendor discovered some anomalous behavior in one or more of the operating system files, and so sent a “fix” in the form of a different version of one of these troublesome files. This would cause relatively little difficulty if only one application vendor performed this service, or if the file modified by the application vendor is used only by that vendor’s application. However, this is often not the case.

20       When another application is installed, that application may include a more recent version of a shared piece of code. One subset of these shared operating system files are called DLL’s (dynamically linked libraries), though they also go by other names. These shared operating system files are often executable, and they expect a fixed number of parameters, certain kinds of parameters, and so on. If the nature of the shared file has  
25       changed (e.g., the parameter set is different, the name is different, the function is different), the calling application may no longer behave correctly. Many common computer functions such as “print” are referenced in this fashion.

Many software vendors try to provide the “latest” version of the operating system file. However, when a different application is loaded onto a computer, it may overwrite  
30       and subtly (or not-so-subtly) change an operating system file that the original application needed to function as planned.

Assume an administrator for an organization is charged with keeping one hundred servers up and running while supporting three thousand users connecting to these servers. The administrator is also responsible for installing user requested or management dictated applications – either shrink wrapped purchases or internally developed applications. The administrator also has responsibility for the timely distribution, locally or remotely, of time sensitive documents.

Now imagine that six service packs must be installed on the network and distributed to all of the clients. Applying the six service packs could easily result in seven visits to each and every one of the hundred servers for a total of seven hundred visits. This number assumes one extra visit per machine because the application of one of the service packs may cause more problems than it fixed, so it had to be undone.

If the three thousand clients were all running the same workstation operating system, that could mean another twenty-one thousand visits to apply the patches. Remember this all has to be accomplished while installing and patching the internally developed applications and the shrink-wrapped products. Distribution of software patches and files and their subsequent application becomes the first indication of what might be called “administrator agony”.

While all the installation is occurring, the individual servers must still be monitored. When a server needs attention the administrator is often contacted by another person, who may frantically report that their server is down and must be fixed. If the administrator had some method to monitor these devices, he or she could become more responsive and further reduce the impact of problems. Monitoring needs are a second indication of “administrator agony”. There is often high turnover in the administrator’s job, and the users of these systems may experience lower productivity.

Traditionally, the administrator had been helped by being given extra staff. Of course this remedy is not without problems – the addition of personnel increases the number of communication channels between them. The people involved in installation and updates need a tracking device or system so they don’t perform or attempt to perform the same unit of work. This lack of coordination between team members is a third indication of “administrator agony”.

Proposed solutions are currently available in varying forms, implementations, and coverage or completeness. Typically these proposed solutions are available as shrink-wrap products that are installable (e.g. patchable) locally in the administrator's environment. Some emerging products are helpful, but many conventional solutions are invasive in that they require massive modification of the administrator's environment. The shrink-wrap solution requires additional invasive full product installations in the administrator's network, thereby adding to the problem, and lacks a central "command center" to coordinate the support or distribution plan. Emerging solutions may provide a somewhat lesser degree of invasion, but nonetheless require a special connection between the administrator and the solution, and they often do not provide a center for coordinated efforts.

Furthermore, it is not always obvious exactly what patches, if any, a given piece of software has received. Updates don't always clearly announce their presence. So, it is not always clear whether a specific computer has previously received a specific patch. Accordingly, there is a need for improved tools and techniques for updating computers across a network. Such tools and techniques are described and claimed herein.

### BRIEF SUMMARY OF THE INVENTION

The present invention relates to methods, articles, signals, and systems for determining if software needs updating, and if so, then updating the software across a network with reduced demands on a human administrator. If the update fails, the computer(s) upon which the update software was installed may be restored to a non-updated state.

In various embodiments, the invention facilitates software deployment, software installation, software updating, and file distribution based on software and patch fingerprinting across multiple operating systems and devices, across a network. Any computer with a network connection and with an update agent running on it may connect to an update server, and then process whatever tasks the administrator has designated for that agent.

Figures 2 shows an overview of one such system. A network 200, shown with only two target computers and an update computer for simplicity of illustration, is protected

from the internet by a firewall 214. The software that is needed to update network target computers 202, 208 resides on package computers 230, 234 that are located inside or outside the firewall and barred by the firewall 214 from direct communications with the target computers 202, 208. However, an update server 220 does have access 216 to the  
5 network 200, potentially through internal firewalls – as well as access through the firewall 214. The system is designed to work both as an onsite purchased solution as well as a fully offsite hosted solution, and can operate through firewalls and proxy circuits at any level within the Intranet/Extranet infrastructure.

Patch fingerprints 902 give a recipe to allow a repository component to determine  
10 if a given software package (associated with the patch fingerprint) , patch, driver, etc. should be loaded onto a computer in the system. These fingerprints are stored in a patch component database location 900 that may be inside or outside the firewall 214. It may be at a separate location or it may be installed on the update server 528. The repository component also includes an inventory library database 918 that contains basic hardware  
15 and software information about each of the network target computers 202, 208. Using the information in the patch fingerprint, the inventory library, and specific information gleaned from each network target computer, the system is able to intelligently recommend which patches and drivers are required for a given computer.

As shown in Figure 5, the preferred embodiment of the invention employs an  
20 additional agent known as the discovery agent 548 installed on the target computer 500, which routinely discovers the hardware and software on that machine. This inventory information is then reported back to an inventory library 918 located somewhere else in the repository component. In addition to the computer inventory, the discovery agents also return scan results for patch fingerprints, which indicate whether it is appropriate to install  
25 a specific patch associated with each patch fingerprint.

The Inventory Database thus collects a complete inventory of the software, hardware and current patch fingerprints that are installed on any particular target computer within the network. With this information, the update server 528 can present the user with detailed reports of the current patch status for all computers within the network. This  
30 illustrates the number of computers needing the patch as well as the computers already installed with the patch.

In addition, Finger Print definitions 906 are also normally associated with an update package suitable for deployment by the system. Once the need for a particular patch has been established by scanning its signature(s) on all computers within the network it can then be quickly deployed by the administrator by merely selecting the date and time.

5       The patches that need to be loaded onto specific target computers are listed on the update server 220 in update lists 222 associated with update agents 204, 210; in the illustration, list 224 is associated with Target1 202, and list 226 is associated with Target2 208. The update lists specify at least one location (through means such as a universal resource locator, or URL) where the patch can be found, and optionally include a date  
10       which is the earliest date that the software can be installed.

In operation, the update agent 204 of Target1 202 checks its update list 224 at the onsite or offsite update server 220 to see if a new package should be installed. If one is there, the update agent 204 checks to see if the package is already in memory on the update server 220. If so, the update agent 204 attempts to install the software patch directly from  
15       the update server 220. If not, the update agent 204 attempts to install the software patch directly from the package computer location 232. In some instances, this is successful, in which case the update list 224 is updated.

In other cases, a download 218 will be obstructed by the firewall 214. If this happens, the update agent 210 informs the update server 220 and then the update server  
20       220 itself will attempt to retrieve the package and place it in memory 228. From that memory on the update server, the software is installed directly to the target machine.

A monitor checks to see that the software installs properly on the target 202, 208, and then continues checking (or can be notified) to ensure that the updated software runs correctly and that the target computer itself doesn't experience any problems in what  
25       appear to be unrelated areas. Should the package fail to install properly, or create problems for the software program that was patched, or create other problems on the target computer, the package can be automatically removed and the computer restored to its preinstalled state or another acceptable state in which the update has been removed or disabled, and the target computer is in a workable state. If the package has been installed  
30       on more than one computer, they all can be removed. If the error occurs in the middle of a rollout to many computers, the rollout can be halted and the software removed or disabled.

The monitor may be located on the update server 220, on a repository site 600, at least partially in the update agent 204, 210, and/or in a combination of such locations.

When there is a problem with an installation, or when an installation is successful, an administrator can be notified by email, by pager, by beeper, or by some other  
5 notification means.

The update agent 204, 210 can also be used to survey its own target computer, and this information can be stored in a database offsite or at another location. This information can then be used to determine what updates a given target computer needs in order to have the most appropriate configuration. When a new software patch becomes available, the  
10 stored information can be used to determine if a particular target computer needs the patch.

Other aspects and advantages of the present invention will become more fully apparent through the following description.

### BRIEF DESCRIPTION OF THE DRAWINGS

15 To illustrate the manner in which the advantages and features of the invention are obtained, a more particular description of the invention will be given with reference to the attached drawings. These drawings only illustrate selected aspects of the invention and thus do not limit the invention's scope. In the drawings:

Figure 1 is a diagram illustrating one of the many distributed computing systems  
20 suitable for use according to the present invention.

Figure 2 is a diagram illustrating systems according to the present invention.

Figure 3 is a diagram illustrating methods according to the present invention.

Figure 4 is a diagram further illustrating methods according to the present  
invention.

25 Figure 5 is a diagram further illustrating systems according to the present invention.

Figure 6 is a diagram further illustrating systems according to the present  
invention.

Figure 7 is a diagram further illustrating systems according to the present  
30 invention.

Figure 8 is a diagram further illustrating methods according to the present invention.

Figure 9 is a diagram further illustrating systems according to the present invention.

5

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides systems, methods, articles, and signals which help update existing software across a remote network. The invention relates more specifically to updating software across a client-server system with little or no need for human oversight, and without requiring copies of the software patches on an administrative machine on the network whose clients are being updated. The update is automatic, and it can detect errors within a specific update and automatically rollback a faulty update to leave the network in a usable state.

Separate figures discussed herein illustrate various embodiments of the present invention, but the discussion of a given figure is not necessarily limited to a particular type of embodiment. For example, those of skill will appreciate that the inventive methods may also be used in configured storage media and/or computer system implementations according to the invention. To prevent unnecessary repetition, the discussion of methods thus applies to articles and systems, and vice versa, unless indicated otherwise. It will also be appreciated that method steps or system components may be renamed, regrouped, repeated, or omitted, and that method steps may be ordered differently and/or performed in overlapping execution, unless the claims as properly understood call for particular steps or components and/or require a particular order of execution.

For the reader's convenience, some pertinent information on related technologies such as networks and firewalls is provided below. The invention goes beyond previously known technologies, but it may partially comprise or rely on earlier advances in computing and networking and/or be used together with such earlier advances.

### Systems Generally

As shown in Figure 1, computer networks 100 such as secure computer networks 102, 104, may be configured according to the invention. Suitable computer networks 100,

102, 104 include, by way of example, local networks, wide area networks, and/or portions of the internet. "Internet" as used herein includes variations such as a private internet, a secure internet, a value-added network, a virtual private network, or an intranet. Secure networks may be secured with a security perimeter which is defined by firewall software  
5 116, 118 routing limitations, encryption, virtual private networking, and/or other means. The network 100, 102, 104 may also include or consist of a secure intranet, which is a secure network such as a local area network that employs TCP/IP and/or HTTP protocols internally. The computers 110 connected by the network for operation according to the invention may be workstations 114, laptop computers 112, disconnectable mobile  
10 computers, servers, computing clusters, mainframes, or a combination thereof. The computer hardware may be general-purpose, special purpose, stand-alone, and/or embedded. The network 100 may include other networks, such as one or more LANs, wide-area networks, wireless networks (including infrared networks), internet servers and clients, intranet servers and clients, or a combination thereof, which may be protected by  
15 their own firewalls.

A given network 100 may include Novell Netware<sup>®</sup> network operating system software (NETWARE is a registered trademark of Novell, Inc.), NetWare Connect Services, VINES, Windows NT, Windows 95, Windows 98, Windows 2000, Windows ME, LAN Manager, or LANtastic network operating system software, UNIX, TCP/IP and  
20 NFS-based systems, Distributed Computing Environment software, and/or SAA software, for instance (VINES is a trademark of Banyan Systems; NT, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS ME, WINDOWS XP and LAN MANAGER are trademarks of Microsoft Corporation; LANTASTIC is a trademark of Artisoft; SAA is a mark of IBM). The network may include a local area network which is connectable to  
25 other networks through a gateway or similar mechanism.

One system according to the invention includes one or more servers 106 that are connected by network signal lines 108 to one or more network clients 110. The servers and network clients may be configured by those of skill in the art in a wide variety of ways to operate according to the present invention. The servers may be configured as internet  
30 servers, as intranet servers, as directory service providers or name servers, as software component servers, as file servers, or as a combination of these and other functions. The

5 servers may be uniprocessor or multiprocessor machines. The servers 106 and clients 110 each include an addressable storage medium such as random access memory and/or a non-volatile storage medium such as a magnetic or optical disk. The signal lines 108 may include twisted pair, coaxial, or optical fiber cables, telephone lines, satellites, microwave  
relays, modulated AC power lines, and other data transmission "wires" known to those of skill in the art, including wireless connections. Signals according to the invention may be embodied in such "wires" and/or in the addressable storage media.

10 In addition to the network client computers, a printer, an array of disks and other peripherals may be attached to a particular system. A given computer may function both as a client 110 and a server 106; this may occur, for instance, on computers running Microsoft Windows NT software. Although particular individual and network computer systems and components are mentioned, those of skill in the art will appreciate that the present invention also works with a variety of other networks and computers.

15 Suitable software and/or hardware implementations of the invention are readily provided by those of skill in the art using the teachings presented here and programming languages and tools such as Java, Pascal, C++, C, Perl, shell scripts, assembly, firmware, microcode, logic arrays, PALs, ASICs, PROMS, and/or other languages, circuits, or tools.

### **Configured Media Generally**

20 The servers 106 and the network clients 110 and individual computers 110, 114 are capable of using floppy drives, tape drives, optical drives or other means to read a storage medium. A suitable storage medium includes a magnetic, optical, or other computer-readable storage device having a specific physical substrate configuration. Suitable storage devices include floppy disks, hard disks, tape, CD-ROMs, PROMs, RAM and other  
25 computer system storage devices. The substrate configuration represents data and instructions which cause the computer system to operate in a specific and predefined manner as described herein. Thus, the medium tangibly embodies a program, functions, and/or instructions that are executable by the servers and/or network client computers and/or individual computers to perform updating, monitoring, administrative and/or other  
30 steps of the present invention substantially as described herein.

## Firewalls

Network administrators generally do not allow just any information into their system. Rather, they use a firewall 116, 118 to protect the network from security threats. A firewall is hardware and/or software device that screens incoming messages (often based  
5 on content, origin, or nature of request) and only allows to pass those that are deemed safe. Three main types of firewalls are screening routers (also called packet filters), proxy server circuit-level gateways, and proxy server application-level gateways. Screening routers can base decisions on external information about a network packet such as its domain name and IP address, so messages that come from acceptable domain names and IP addresses  
10 can be allowed through 120, 124 while refusing messages from other locations 122. Proxy server circuit-level gateways disguise information about an internal system when passing the information to an external system. The IP addresses of the internal computers are typically replaced with the IP address of the proxy. At this level, authentication can be required. Proxy server application-level gateways provide all of the features of screening  
15 routers and circuit level gateways while also allowing the contents of the packets themselves to be evaluated. Messages can be rejected for content as well as for security violations.

## Software Installation

20 System administrators often need to change the software on a specific machine. A new piece of software must be installed for the first time, as when a new application is added to a machine. An already-installed piece of software can be updated, as when a new version of an existing piece of software will be installed on a specific machine; this is also referred to as "replacing" the software. A data file of an existing piece of software can be  
25 updated without otherwise changing the software configuration, as when tax tables are updated on an accounting program, or when anti-virus software files are updated. If a problem is discovered in an existing piece of software, then a fix or patch can be installed. Any or all of these changes to the state of a specific machine or machines are referred to in this patent as "installation". Similarly, the words "package," "patch," and "update" should  
30 be given the broadest possible meaning. For example, package could refer to an entire program including all the necessary files, to one or more data files, to a software patch to

an existing file, to a change to a configuration file, to a \*.dll file, a driver file for a specific piece of hardware attached to a computer and/or a computer network, and so on. "Update" refers to at least attempting to install a package on a computer.

## 5    **Methods Generally**

With reference to Figures 3, 4, and 5, one embodiment of a method operating according to the present invention includes a target computer 500 in a pre-update state. The target computer 500 is the computer that the invention will at least attempt to update; not every embodiment of the invention requires that the update be successful. An update  
10    server 528 is connected across a network 524 to the target computer. In some implementations the target computer has a non-graphical user interface network connection, such as a connection through a winsock layer. Typically, the target computer is protected by a firewall 526, as explained above, but the update server can drill through the firewall to access the target computer.

15        An update agent 508 is located at each computer that is to be updated. The update agent is a software component (usually not very large) that may be installed initially, either in the traditional manner or by using the invention, on the network target machines such as workstation(s) and/or server(s). The update agent is capable of operating in the place of the human administrator, at the direction of the human administrator, to perform work in a  
20    manner similar to what could be performed if the human administrator was actually present at the machine. The update agent knows how to perform two basic tasks: 1) how to contact the update server 528 to retrieve a list of tasks and 2) how to start the tasks in the task list received.

The update agent is capable of updating, configuring, or replacing itself without the  
25    need for manual intervention after the initial install. Typically a small boot-strap agent will be installed initially, but will grow in abilities as the administrator dictates or as required to fulfill administrator requests. The update agents of different sorts of target computers 500, such as onsite administrator computers, server computers, and client machines, can all start out as the same version of a single agent. Machines in a given network can all  
30    have a the same agent installed, or machines can have unique agents installed. When there is more than one client, each can have a different update agent initially, or a mix of agents

can be installed on different client machines, as is chosen by the administrator, or as is set up as a default. Similarly, multiple servers and administrators can also have a mix of different agents initially installed. As the agents for the individual target computers change, they can all change in concert or they can diverge. In some embodiments, the agents may all start out different and then converge in functionality.

The offsite location of the update server 528 is a location distinct from the target computer. The location may be offsite at a completely different vendor, or offsite at a different physical location from the target computer 500 but at a location managed by the same entity, at the same physical location. It may be at a different-appearing location from the target computer 500, such as at a subcontractor location, or at some other distinct-appearing location. The important point is that as far as an individual target computer operating system is concerned, the work appears to be off-site. One embodiment locates the update server on the target computer 500 but in a fashion (such as in a different partition) that appears offsite.

The actual update material that is to be installed on the target computer is often stored at a separate location (known as the package computer) apart from the update server and the target computer. The software update itself can be any of a wide variety of software that can be updated across a network, such as an incremental software patch, a new software program never before installed on the target computer, an update to an old program, software scripts, data files, or even an update of the update agent.

If a known condition is met, during a placing step 300, a task id is placed on an update task list 222. The known condition could be that the patch is not currently on the computer, that the administrator has given assent, the owner of the target computer 500 has permission from the owner of the package, the fact that no one has specifically denied placing privileges, or some other known or inventive condition. The update task list located on the update server is associated with a specific target computer 500, and specifies at least one download address where the software update can be found. The download address can be in any format that is understandable to the computers. The invention does not depend upon any specific addressing convention. Two common addressing formats in use currently are the "Universal Resource Locator" and "fully qualified domain name" formats. Other formats are PURLs (Persistent Uniform Resource

Locators) and URN's (Uniform Resource Names), and other naming schemes may be known in the future. Other information that may be included in the task identifier, such as a date the download will first be attempted. Multiple download addresses, each of which specifies a location where the software update can be found, may all be associated with a  
5 specific software update.

During a starting task step 304, the software update is at least attempted to be uploaded from the package computer 567 to the update server 528. During an optional choose package computer step 306, if more than one download location is placed on task id list 226, the location that the software update will be downloaded from is chosen. The  
10 choice can be made by any known or inventive method, such as using the first location on the list, using the location that a test message returns from most rapidly, using the first available machine, and so on.

Once a location for the update is known, the software download is attempted from the location of the package computer 548 to the memory 530 of the update server 528. If  
15 the download is unsuccessful, then in one inventive method another location from the list of possible locations in the task update list is chosen, and the download of the software update is retried. In some implementations, if the download can't be completed for some reason, the update server 528 waits for a time and tries to download from the package computer 567 again. If the download is successful, then the update server 528 attempts to  
20 download 312 the software update to the target computer 500.

Once the download is in cache or other memory in the update computer a second download 312 is attempted to download the software package from the update server to the target computer. In some embodiments of the method, the second download 312 is delayed  
310 by some predetermined criterion. This delay may be from the start of the first  
25 download, with the delay period based on an estimate of the time needed to download the software update from the package computer to the update server. The second download may also be delayed to a specific time of day when the target computer 500 has less of a chance of being used, such as after a business closes for the day. Other known or inventive delay criteria may also be used.

30 A monitor 302 checks the installation, performing the role typically played by an administrator, to determine the results of the installation 314. Once the results are known,

an administrator can be notified 328. Notification can be by sending an email 330, by paging someone, by sending a pre-recorded phone message, or by any other known or inventive method and means.

If the monitoring step detects a failure 316, then the task that failed is suspended 318. The first download 308 to the update server 528 could fail, as could the second download from the update server 528 to the target computer 500. If there are multiple target computers having the software update installed, the Nth installation could fail, and so on. Determining results preferably goes beyond simply ensuring that the software update appears to have installed properly, and in some embodiments of the invention extends for a time beyond the installation. For example, one embodiment of the monitor will test a patch application by having it installed it on only one target computer, assuring that it downloads properly, and then watching it for some period of time until the administrator who sets the time delay gains enough confidence in the patch to allow it to be applied to other target computers. Should the application of this patch cause abnormal activity, as noticed by undesirable behaviors either in the program whose software was modified or elsewhere in the computer, the rollout can be automatically discontinued until the problem is resolved.

Furthermore, in some instances when failure is detected the software update is disabled or removed 324 from the target computer, and that machine is returned substantially to its pre-update state or another acceptable (working) non-update state. This may mean that the installed software is taken off the target machine 322; or that not only is the software removed, but all the ancillary files (.dll's, .exe's, etc.) are restored to their pre-update state. In other instances it may mean that the target computer or some portion thereof was backed up before the software update was installed, and the backup itself is restored onto the machine.

If there are multiple target computers 500, failure may be detected by the monitor after the software has been installed on one or more machines. In this case, the software update can be removed 322 from not only the target computer 500 where the failure was spotted, but it can also be removed 326 from all of the other target computers 500 where the software was previously installed 326. The removal request can come from an administrator or removal can be performed automatically after failure is detected 316.

The monitor 302 may perform more tasks than simply waiting to hear if a software package has installed successfully. For example, in some instances the monitor waits for a time period 400 after the installation and if it has not heard otherwise, assumes that the installation was successful.

5           Administrators and administrator helpers can benefit greatly from a central repository where they can enter and retrieve information regarding requests for help. One such method is help desk "ticketing". Ticketing records the requestor, the type of request, when help was requested, when the response to the request was completed, and other useful information. A PatchLink HelpDesk service provides facilities for administrators to  
10   manage their network requests and network resources, both people and computer resources, via one central repository. PatchLink HelpDesk software provides these facilities across the internet without an invasive application install on the administrator's network that introduces yet another resource that has to be managed, backed up, and updated – this is taken care of transparently at an offsite Management Center.

15           A website, reachable by a standard web browser or some other known or inventive network connection, provides the facilities to use the help desk services. A preferred implementation is currently at the PatchLink web site, reachable at [www.patchlink.com](http://www.patchlink.com). Simple web forms support the data collection required to begin the enrollment process. Once the enrollment process is complete, the administrator can license one or more  
20   services on a recurring subscription basis.

          The enrollment process is begun when the administrator initiates the process by signing up and indicating a desired level of participation. A preferred embodiment of the invention has three different user levels: guest, regular, and executive. A guest is allowed to view the web site and can read the user forums but cannot post to the forums. A regular  
25   member can perform guest functions and can also chat in chat rooms, and post to forums. An executive member has a subscription to the site. He or she can perform regular member functions, and can also use the more advanced features of the site, such as offsite automatic package updates (e.g., PatchLink Update services), offsite monitoring (e.g., PatchLink Monitor services), and the offsite help desk functions (e.g., PatchLink  
30   HelpDesk services).

One embodiment of the method entails an email being sent to a customer care agent assigned to the customer's telephone area code. The customer care agent telephones the pending user to complete the enrollment process. The customer care agent collects the necessary identity information and payment information, and then upgrades the pending  
5 user's account to permit use of the account, making the pending user an administrator/  
user. The areas the administrator/user can participate in or use is controlled by entries in the licensed product's table of the update host's database. These entries are created by the customer care agent during the enrollment process.

Recall that all these services are available to the administrator via a browser or  
10 other network connection across the internet. When a monitor enters a ticket into the help desk and initiates a rollout in some instantiations of the inventive method, the monitor then decides whether a failure has occurred 316, 406. To decide the monitor may look at what software updates have recently been installed, how long ago the installations occurred, the current hardware and software configuration, and so on. Which incidents are considered  
15 failure can be, without limitation, set by an administrator; defaults can be used, and judgment of the help desk personnel can be taken into account.

In a detect success step 408 the target computer 500 sends a message 410 to the update server after the download from the update server to the target computer has completed successfully. The monitor can presume success 404 if a specified time period  
20 has passed without noticing or being notified of a failure.

Failure can be detected in other ways 316, 406. For instance the target computer can notify the monitor that a failure has occurred; a user can notify the monitor through the help desk or through a direct link that a failure has occurred; when a target computer does not contact the monitor within a specified time from the beginning of the second download  
25 312 onto the target machine, a human administrator can declare that a failure has occurred; and so on. Notice that even after the monitor has declared the outcome of a download to be a success, later events, such as an indication of failure from the help desk, can cause the monitor to declare the download to be a failure.

In one embodiment of the invention, the update server 528 waits for a confirmation  
30 of a successful installation (by the monitor, or by another known or inventive contact method) before the next target computer 500 has the software update placed on its update

list 222. The update server checks for a target computer 500 that is eligible for the software update but has not yet received it 412. If one is found 414 the appropriate task identifier, specifying the target machine, the software update, and the location, are added 416 to the update server's 528 task update list. This way, rather than a mass update where  
5 all eligible computers have the software installed on them *en masse*, the rollout proceeds one computer at a time until, after a default or user-defined number of successful installations, the rollout is deemed a success; at that juncture the software update is made available to more than one target computer at a time.

It is not always clear by looking at a specific target computer 500 what software  
10 packages and patches have been installed. The invention includes a method to analyze a target computer 500 to ensure that a given patch has not already been installed on the computer 500 before the invention attempts to install that patch. The following discussion includes references to Figures 8 and 9 and continuing reference to Figure 5.

A patch fingerprint which defines a specific software update is described in greater  
15 detail below. The patch fingerprint is located 800 by monitoring a patch component database location 900 for a new patch fingerprint 902. The word "new" here indicates that the patch has not yet been downloaded into the repository component 600, or for some reason needs to be downloaded into the repository component again, even though it has been downloaded previously. There may be one or many patch component locations; those  
20 locations may be on a separate computer connected to the system through a network link, on the update server 528, on the target computer 599, on the package computer 567, on a non-networked location such as a CD, a tape, a floppy disk, etc., or some other known or inventive location.

Once the patch fingerprint 906 is located 800, it is placed 802 into the repository  
25 component 600. The usual method of placement is to download 804 the patch fingerprint 906 into the repository component, but in some embodiments the fingerprint 906 will be on the same file system, so the patch fingerprint will be copied without using the network, such as copying between partitions.

The illustrated patch fingerprint comprises one or more general inventory install  
30 dependencies 912 that can be used to take a high-level look to see if a specific patch can be installed on a machine. It also includes a signature block 910 that can be used to request

specific information from a target computer 500, and an existence test 908 which can use the signature block information to determine if a specific patch has been loaded on a machine.

In some versions of the invention, the inventory install dependencies 912 describe  
5 at least some of the necessary software and hardware that must be installed on the target computer 500. These dependencies 912 are compared 808 with information about the target computer 806 previously stored in the inventory library 918. If the install information and the inventory information don't match, then the patch is not installed. In some versions of the invention a message is sent to at least one administrator containing a  
10 list of components required (such as necessary hardware and software) for the install.

If the necessary inventory information is on the target computer 500, or if the inventory info is not used, then the signature block is sent 810 from the repository computer 600 to target computer 500. The information requested in the signature block 814, which may consist of more specific install information, is gathered 812 by the  
15 discovery agent 548 and then sent back to the repository component 818. In some versions of the invention, the discovery agent also gathers other information 816 about the target computer such as usage statistics, hardware and software installed, configurations, etc. This information can then be used to populate the inventory library 918.

Once the signature information 910 has been sent to the repository component 600,  
20 an evaluator 914 evaluates at least a portion of the specific install information requested by the signature block using the existence test 908, and in some instances the inventory install information 912, to determine if the patch is absent 822 on the target computer 500.

As an optional step, once it has been determined if the patch is absent a message is sent 824 to at least one address associated with an administrator. This message may be sent  
25 using a variety of methods, including email, pager, fax, voicemail, instant messaging, SNMP notification, and so on.

### **Patch Fingerprint**

With continuing reference to Figures 5, 8 and 9, one embodiment of the system  
30 verifies that a software package can reasonably be installed on a given target computer 500 before attempting installation. To do so, a patch fingerprint 906 is used. It defines how to

determine if a given software package/incremental patch has been previously installed. It may also define a minimum hardware/software configuration necessary for the patch installation. These patch fingerprints 906 are stored in a fingerprint library 904. The fingerprint library 904 is located on a repository component 600. This repository  
5 component 600 may be located on the update server 528, or may be in a separate location accessible to the update server 528 and the target computer 500. Some versions of the invention also include an inventory library 918 which contain target inventories. Each target inventory 920 contains the hardware and software information about a defined set of target computers 500. This defined set may include as few as one computer or as many as  
10 all of the computers in a given network, or some number in between.

The fingerprint library 904 can be automatically replenished. In some embodiments, at least one, but possibly several, patch component database locations 900 are monitored 800 for new patches 902. In some embodiments of the invention a signal from the locations 900 indicates to the repository component 600 that new patches 902 are  
15 available 800. In the preferred implementation the fingerprint library 904 is updated with new patch fingerprints at specific time intervals. After the repository component 600 is aware of the new patch fingerprint, the patch fingerprint is placed into the repository component 802, usually by using a downloader 924 to download the new patch fingerprint. Patch fingerprints may be entered into the repository components in other ways, however.  
20 For example, one or more patch fingerprints may be manually installed into the fingerprint library by an administrator.

### **Inventory Library**

The repository component 600 also contains an inventory library 918. A discovery  
25 agent 548, which in some embodiments initially resides on the update server 528, is installed from the update server 528 to the target computer 500 using known or inventive methods. This discovery agent 548, described in greater detail below, inventories at least some of target computer 500's software information 606, hardware information 608 including specific software updates and patches installed, usage information 604, registry  
30 information 612, web information 610, configuration information 614, services 618, file information, patch signatures which have been utilized, etc.

This information, or a subset or superset thereof, is then sent, in some embodiments in compressed form, to the target computer inventory 920 in the inventory library 918. Result information can be quite voluminous, and hence may be compressed for efficient upload and to minimize bandwidth usage on the customers network. A preferred  
5 implementation sends the data using an XML data transfer, though any other known or inventive data transfer method can be used.

### **Report Generator**

With this information, a report generator 922 can present a user with detailed  
10 reports of the current patch status for all computers within the network, illustrating the number of computers needing the patch, the computers already installed with the patch, computers that can't receive the patch until hardware or software is upgraded and so on. In addition, the report generator 922 can provide a partial or complete inventory of the computers attached to the network. In some embodiments the report generator 922  
15 provides graphical presentations of the inventory for analysis by the administrator, both to track location of hardware as well as to ensure software license compliance. However the repository component 600 also uses the inventory library 918 information as well as detected fingerprint information to distribute relevant signatures 910 from the patch fingerprint 906 to the discovery agent 548, thus greatly optimizing the patch discovery  
20 process by eliminating unnecessary scanning work at the target computer 500.

### **Discovery Agent**

One optional step to decide if a given software program or patch can be installed is by verifying that the necessary hardware, if applicable, is present, and/or the necessary  
25 software is present. For example, some programs may require a specific operating system, some programs may require a certain processor. As an example, if an update of Microsoft Word software is to be installed, it is necessary that Microsoft Word software be on the machine. These high-level dependencies are stored, in some versions, in the inventory install block 912 in the patch fingerprint. The information in the inventory install block is  
30 generally high level enough that it can be pulled out of the target inventory 920 of the specific target computer 500 stored in the inventory library 918.

In some implementations of the invention the patch fingerprint 906 also includes installation dependency information 912. This, as explained above, is information about the target computer 500 that can be expected to be found in the inventory library, and so can be checked without querying the target computer 500. This includes software that  
5 should be present (such as a specific version of a program, a patch, a data file or a driver) a hardware component that should be present, or specific hardware and/or software that shouldn't be present.

If the inventory library does not have an up-to-date inventory for the target computer 500, the discovery agent can be used to scan the target computer 500 for  
10 inventory information; it does not necessarily need to also scan simultaneously for signature information. In the preferred implementation, the first time that the discovery agent 548 runs on a given target computer it scans only for inventory information and then loads that information into the inventory library 918; it ignores the patch fingerprint information. At other times when the discovery agent 548 runs it may ignore inventory  
15 information and may, rather, be used to look up specific signature information 910 to test for the existence of a specific patch. When the signature block information is looked for, values such as registry entries and INI file values may be inspected for existence, or the actual value may be returned to the repository component 600.

Each Patch fingerprint comprises a signature block 910 and an existence test 908.  
20 The patch signature block is a set of information requests, the information itself to be gleaned from a target computer 500 which will then be used to determine if all necessary bug fix and security patches are installed. Examples of patch signature block information include but are not limited to file, hardware, registry and configuration information, a specific file name or directory name, all or part of a path that a file is expected to be found  
25 in, a specific version of a file, a created date of a file, a file version, and a specific registry value.

In one implementation the fingerprint library 904 is a SQL database. The patch signatures 910 are extracted from the SQL fingerprint library and then sent to all target computers that meet the dependency criteria for operating system and installed software as  
30 specified in the inventory install information 912.

A preferred implementation employs an XML-based request input file. The result file sent back to the update server 528 also employs XML formatting. This result file contains the signature information for the target computer, and may also contain the software and hardware inventory updates. The inventory and signature information sent to the update server can be quite voluminous, and so are compressed in the preferred implementation. The following is a sample patch signature that will gather registry information for Microsoft Outlook as well as the EXEs date and time, and information in the registry :

```

10  <file componentid="1" reportID="1">
      <name>outlook.exe</name>
      <path></path>
      <version>9.0.2416</version>
      <created></created>
      <size></size>
15  <root>HKEY_LOCAL_MACHINE</root>
      <Key>SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\OUTLOOK.EXE</key>
      <value>Path</value>
    </file>

```

Once the discovery agent on the target computer has returned its scan results for the signature, the existence test 908 logic is used by the evaluator 914 to infer whether that particular computer actually has the patch or not. This algorithm minimizes the number of tests that must be done by the evaluator: its sole responsibility is to discover information – allowing the data analysis to be done by the repository component 600 itself. Distributing the workload in this fashion provides a better implementation for scanning and analyzing huge numbers of workstations and servers.

Each existence test is specific to a given patch. A sample existence test might appear as: if registry QQ contains value ZFILEVAL or (if file \_Z123.bat was changed on date 12/12/2000 at 11:52 pm and file Z is of size ZFILESIZE) then the patch ZPATCH is present. The preferred embodiment of the patch fingerprint library is an SQL database, but other known or inventive databases can be used.

Note that a patch fingerprint may also contain dependencies to other Finger Print definitions: for example, “MS-023 IIS Vulnerability Fix” patch might hypothetically require the presence of “Microsoft Windows Service Pack 2”. This is used to further optimize where the patch signatures are actually sent. These may sometimes be used in the

install dependencies info 912 and other times in the signature block 910, depending on circumstances.

In addition, fingerprint definitions 906 are also normally associated with a software package 554 suitable for deployment by the system. Once the need for a particular patch  
5 has been established by scanning its signature(s) on all computers within the network it can then be quickly deployed by the administrator by merely selecting the date and time.

In some implementations the downloader 924 regularly checks the patch component database for new patch fingerprints. When a new patch fingerprint is located, it is downloaded into the repository component. The evaluator compares the dependencies  
10 needed for the specific patch implementation listed in the install info 912 with each of the target computer 500 specifications listed in the inventory library. Then an update list is created which may identify all of the target computers 500 that need the patch, all of the target computers that don't possess the patch, all of the target computers that can receive the patch, as they have the necessary dependencies, and/or all of the target computers 500  
15 that have already received the patch. This update list may now be used to update the target computers, and/or may be sent to an administrator by a notifier 916.

In some instances of the invention the patch component database is owned by someone other than the target computer 500 owner. Only if this patch update host has given permission to the target computer 500 owner will the downloader be allowed to  
20 download the new patch fingerprints into the repository component. The permission may comprise a purchase agreement, a lease agreement, and an evaluation agreement.

If any modifications are made that may be of interest to the administrator, the notifier 916 will send a notification message containing the new patch updates that have become available or the patch-related state changes that have occurred in his network  
25 configuration. Notifications can be sent via e-mail, pager, telephony, SNMP broadcast or Instant Message.

### **Target Computer**

In one embodiment, the inventive system comprises three pieces: a target computer  
30 500, an update server 528, and a package computer 548. The target computer 500 has a memory 502, and a network connection 504, which in at least one implementation of the

invention is a winsock layer but which can also be a browser. A socketless protocol can be implemented, or any other known or inventive network connection can be used. The update server 528 has a memory 530 that may include an optional backup storage 534, and a network connection 532 which may be a browser. The package computer 567 has a  
5 memory 550, and a network connection 552 which may be a browser. Figure 5 shows one target computer 500 for convenience but there may be many more in a given embodiment. Likewise, one update server 528, and one package computer 567 is shown for convenience, the invention may only require one but also support two or more. In a preferred embodiment these pieces are all separate computers, but they can be virtual  
10 pieces of the same computer, such that they appear to be distinct. For example, the "package computer" piece may reside on a different partition of the update server.

The target computer contains a network connection 544, which may be protected from the outside by a firewall 526 as is discussed above. Different target computers within a network may run on different platforms; for instance, some may be Windows machines,  
15 some Unix machines, etc. The same update server 528 can be used for all the platforms, or different update servers 528 can be specified by platform type, or the update servers 528 can be assigned to target computers 500 using a different schema.

The target computer 500 also contains an update agent 508. The update agent is a software component that can be installed using the inventive method on multiple machines  
20 at a time or, in some embodiments of the system, can be installed in the traditional manner on the target computer 500. The update agent 508 knows how to perform two basic tasks: 1) how to contact an update server 528 to retrieve its list of tasks from its update list 536 and 2) how to start the tasks in the task list received.

## 25 Update agent

The update agent of target computer 500 contacts the update server 528 to determine if there is work for the agent 508 to do. The update server 528 determines this by analyzing an agent's update list queue 536. This update list 536 contains, at a minimum, a software location reference 538, but can also contain a date 540 that indicates  
30 the earliest date that the software package 554 can be installed, and multiple software location references, if the same software package is available from multiple locations. The

types of software 554 that can be updated comprise, without restriction, patch files 556 that update a currently installed software application on the target computer, data files 558, script files 562, new application files 564, executable files, 560 and updates to the update agent file itself 566 .

5       When the update agent discovers an entry on its associated update list 536, with an appropriate date 540, if any, the installer 510 initially checks to see if a copy of the software package already exists in memory 530 on the update server 528. If found, it then downloads the software package directly from the update server. This situation may arise when a previous target computer 500 has requested the software package 554 from the  
10       update server 528.

      If the software package is not found, the installer 510 then attempts to download the update directly from the package computer location given in the software location reference 538 to the target computer memory 502 using its network connection. This will be possible if there is no firewall 526, or if the update server can browse the package  
15       computer location 548.

      When an administrator builds a package that instructs the update agent 508 to retrieve the files from a "non trusted" source such as the package computer 567, the installer 510 will be unable to retrieve the resource directly. However, the update agent can ask the update server 528 to retrieve the package. In some implementations there are  
20       multiple update servers and the update agent 508 decides which one of them to access using some predetermined criterion. Examples include selecting the first update server 528 that is available, selecting the least-busy update server, selecting the update server that is "closest" in networking terms, and so on.

      In one implementation of the invention, if the update server 528 can reach the  
25       offsite package computer 567, it reports to the update agent 508 that it can reach the resource and estimates the time the retrieval will take. This estimate informs the agent how long it should wait before the requested resource is available. If the calculation estimation is not exact, as it probably will not be because of internet traffic fluctuations and server response time variances, then if the agent asks for the resource again the update server will  
30       provide another wait time length and the agent will wait once again. This cycle will repeat

until the update server 528 has the resource available in memory and can deliver it to the agent upon the next request.

As a particular software package could be requested multiple times by different agents 508, in one implementation of the invention, the update server 528 will store this resource in a local cache 530 from which it can fulfill additional retrieval requests. To prevent the update server 528 from filling up all its available memory with old software packages, one embodiment stores the number of times the package is accessed and the time of the latest access for the stored software package and estimates a "time to live" amount of time for that resource to stay in its cache. A separate task running in the update server 528 will check periodically for resources that have "outlived" their usefulness and recover the update host's storage resources by deleting the stored software package update from the cache 530.

In one embodiment the update server will make the packages available to the list of agents one at a time. If an agent 508 or an outcome finder 512 reports that the application of the patch failed, or if the patch puts the agent's target computer 500 in such a state that it can no longer communicate with the update server, then the update server will suspend the rollout automatically on the administrator's behalf. At this point, the administrator, or some other designated person can be notified 516 of the outcome.

An outcome finder 512 determines if the software package installation was successful and then communicates its finding to the update server 528. If the outcome is unsuccessful, as discussed above, a restorer 514 places the target computer in an acceptable non-updated state. The outcome finder 512 does not necessarily monitor only the actual software installation; rather it can be set up to watch uses of the software that was patched, the entire target computer, and/or computers that are networked to the target computer, for some designated period of time. The outcome finder can also have different levels of success. For instance, the installation itself (file copying) can be considered a low level of success, while the target computer not misbehaving for a period of time thereafter can be considered a higher level of success, with different actions taken according to the success level.

Some embodiments store a backup 506, 534 of a target computer 500 or a portion thereof before installing the software package on the target computer 500. Sometimes the

backup is stored 534 on the update server, sometimes on the target computer 506, 500 which is having its software updated, and sometimes it is stored offsite at a repository site 600. When the outcome finder 512 reports a problem with a software installation, the restorer 514 can use the backup 534 to return the target computer to a non-updated state.

5        In one embodiment of the invention, the update server 528 waits for a confirmation of a successful installation (by the outcome finder 512, or by another known or inventive contact method) before the next target computer 500 has the software location reference 538 to the package placed on its update list 536 at the update server 528. In a preferred embodiment, when an installation finishes, an administrator is notified 516 of the results  
10 by email 518, pager 520, voice mail 522, SNMP notification 568, instant messaging 570, beeper, fax or by some other means. If the installation failed, the specific machine that the installation failed on may be identified. In some embodiments, after a default or user-defined number of successful installations, the package is made available to more than one user at a time.

15        These update lists 536 facilitate the administrator's designation of pre-build packages, or custom build packages, to be delivered or rolled-out to managed workstations or clients and managed servers, which we refer to as target computers 500. When these packages are to be made available, updates are scheduled by the administrator to be performed by the invention; this may automate a previous task requiring the  
20 administrator's visit to a client to install a patch or service pack.

      The update agent 508 may be aware of the platform it is operating upon, and may be programmable or scriptable to perform actions on behalf of the administrator. In one implementation these features are exposed to the administrator through Package Builder wizards. A "software package" can be any combination of files, service packs, and scripts.  
25 This presents an opportunity for the administration of remote machines, since almost anything that could be performed at a remote machine can be accomplished via the agent acting on behalf of the administrator.

      One implementation of the invention allows scripts 562 to be run before (pre-install) and after (post-install) the package installation. An example of a pre-install script  
30 may be: (in pseudo-code)

      check for available disk space

If disk space available greater than ValueX (where ValueX = room needed for install plus a buffer) then start the install.

Else, alert outside administration that an error has occurred, and terminate.

5       An example of an post-install script (again, in pseudo-code):

If install was successful, then notify an outside source that install successful.

If install was unsuccessful, then notify an outside source that install was unsuccessful.

10       Referring now to Figures 6 and 7, the network 200 may include many different sorts of target computers, each with an agent that may be specifically constructed for the specific target platform. For example, a network running Microsoft Windows PCs, Apple computers, and UNIX computers, may have three types of agents. This provides a benefit in that the agent is capable of surveying its target computer and reporting this computer  
15       information 602 to the update server 528 and/or to a separate repository site 600 for storage. In some instances of the system, a discovery agent 548 is provided which performs the scan, as discussed elsewhere. In other instances the scan is performed by the update agent 508, or a downloaded script file 562. Hardware configurations 608, software configurations 606, information about the usage of various hardware and software  
20       components 604, web sites visited, emails sent and received 610, can all be sent to the offsite location 600. Once this information is available at the update server, an administrator can view the entire managed network from one place.

When the inventive system is implemented on an existing network, the discovery agent 548 may perform a survey of the software in existence at least on the target computer  
25       500, with existing software configurations 700 detected and stored within the repository site 600 memory. Some systems may survey the entire network 200. When updates are called for, the system knows which ones are needed without needing to resurvey the network machines to check their current status.

A recommended configuration 704 for the target computer 500 is placed on the  
30       update server 528 or on the repository site 600. The recommended configuration may be decided on in many ways, either inventive or known to those of skill in the database arts, for example, by hardware configuration, by software configuration, by type of computer, by last package update, and so on. The discovery agent 548 then compares the current 700 and recommended 704 configurations and prepares a proposed list of updates 708 for the

target computer 500. The update list may include service packs for installed software, previously uninstalled software, updated data files, and the like. The process of preparing the suggested list may take into account not only the current software configuration but also information such as the hardware configuration 608, and how often a particular  
5 program, data file, etc. is accessed 604, as well as other information that is known to one of skill in the art. An administrator may be automatically notified of the update list.

Assuming that the target computer current configuration 700 generates a proposed update list 706, an administrator may be automatically notified 708. At this point, the computer use may be restricted until the new target computer is updated at least partially,  
10 until the administrator gives permission, or until some other inventive or known condition is met. This proposed update list 706 may also be used to define an update list 536 used to actually update the computer, as explained elsewhere.

Packages are composed of modules representing files, e.g., software files or data files, and scripts, which are sequences of actions to take upon files in the package. In some  
15 embodiments of the invention, a human administrator receives notice of the availability of new software patches. In other embodiments, the notices are sent directly to the offsite update server 528 which decides when to roll them out. The offsite update server can be configured to store in permanent memory the packages that have already been stored on each target computer. When a new package becomes available, or during the installation of  
20 an existing package, existing evidence of the software packages that need to be installed, as well as information about previous installations, is available in some embodiments at the offsite update server 528, and in other instances at the repository site 600.

The packages that are to be updated do not need to be owned by the target computer 500 user to receive access to it. In one embodiment of the system, the software  
25 package is owned by a third party which leases the software to the user. In another embodiment, the software package is owned by the update server user who then leases and provides access to the software package to the target computer 500 user.

### **Implementation notes**

30 Additional details regarding particular embodiments are provided below. These implementation details are provided in order to err -- if errors are made -- by including too

much information rather than including too little. Applicants should not be penalized for being so forthcoming. In particular, the inclusion of details should not be viewed as an assumption or admission that those details, or similar details, or a similar level of detail, are actually required to support the claims ultimately granted. Nor should the inclusion of particular implementation details be misinterpreted by treating as inventors people who simply implemented inventive ideas conceived by others.

#### Agents

- Microsoft Windows Agents
- NetWare Agent
- 10   • Linux Agent
- Java Agent

#### Package Construction / Package Maintenance

15   An administrator uses this module to create a package for distribution through the designated Update agents. This package can be a file distribution or a software package, allowing for more flexibility when updating existing installed software, installing new software, file-replication, etc. throughout the designated managed machines.

Below are the steps for proper package creation:

- 20   1.   Enter the Package Specifications
  - Package Name – Labels the package throughout the updating process.
  - Package Type – When Software Package is selected in the Software Package routines, after the source files for the package are placed in their proper destination sequence, the administrator may immediately finish the package creation (using pre-designated default values for the rest of the options). File Distribution requires the administrator to complete all steps in the package creation routine.
  - 25   • Operating System - Choose the Operating Systems to which the package can be rolled out. Currently, you may select one operating system per package. These include: Linux , NetWare, Windows 2000/NT, Windows NT, Windows 95/98/ME
  - 30   • (Optional) Import – Imports a previously exported package. This option is useful for creating the same package for multiple operating systems.
2.   Add the Source
  - 35   • Add File – Adds a file from your local workstation or network location that is reachable.
  - Add Dir – Adds a directory from your local workstation or network location that is reachable.
  - Add URL – Adds a remote file to the package via well-known protocols. The various types of URLs you can add are: Local File – File://, FTP – ftp://, HTTP – http://, Secure HTTP – https://, Anything else you choose as long as the agent recognizes the protocol (this field is editable).
  - 40   • Remove – Removes a file from the package.

- Properties – Shows the details of how each file is stored within the update server. Also allows for multiple sources in case one source is busy or slow (due to net lag for example). The agent automatically tries the other sources.
- Import File – Imports a specific list of files from a previously exported package.
- 5    3.    Add the Destination
  - Target Computer – A hierarchical tree view of the package file destination. The various default directories shown depend on the operating system for which this package is targeted. The package always displays in the same directory path from which the source files were originally imported (see Step 2). To move the files around simply highlight the directory or file and drag it to its new location.
  - 10    • Properties – If the directory where the files should install is not displayed, highlight a file and click the Properties button. This displays the base information of where the source file is coming from and an entry field for the destination. Type the new location and click OK and your changes are shown (this may take a while because the paths are reconnected for large package file numbers).
  - 15    • Export File – Exports a base package to a file (source and destination information) for use later in an import function.
- 4.    Dependencies
  - Left Column – A list of existing packages that are ready for rollout (operating system dependent). For example, if you have a Java-based package that must be rolled out to numerous computers, you would select the specific JDK package as your dependency so that the JDK is installed prior to the current package.
  - 20    • Right Column – The packages placed here (by using the arrow buttons) are the dependencies for your package. Use the + and – buttons to arrange the dependencies in order of importance (most important being the first dependency). Dependencies are processed before your package.
  - 25    • Asset – If the dependencies are not found the package fails to install. For example, if a Microsoft Office 2000 SR1 package is created, its Asset dependency is Microsoft Office 2000 which must already be installed.
  - 30    • Install – If the dependencies are not found, install them prior to installing the current package. Using the above example, if MS Office 2000 is not found, it is installed prior to installing the SR1 package.
- 5.    Package Settings
  - Backup – Backs up any existing package files found on the destination machines. The editable pull-down list contains the most common directories for the operating system in question. If your directory is not found just type it into the list.
  - 35    • Confidence Level – The default for all new packages is New. The Confidence Level indicates that this package was tested and its performance has determined its confidence level.
  - 40    • Availability – The default is Available which indicates the package is available for rollouts. Not Available indicates this created package is unavailable for a rollout.
- 6.    Scripts
  - There are three types of package scripts you can use: Command Line – The contents of this script are executed as a standard command line. This script is sent after the files are copied to their destinations. Pre-Script – The contents of this script are executed prior to the files being copied onto the machine. Post-Script – The contents of this script are executed after the files are copied onto the machine.
  - 45

## 7. System Settings

- Language – Select the languages for which the package is available. The agent then checks that the language is on the machine and that the package matches before the package is installed.
- 5     • Processor Type – Select the processor for which the package is available. The agent then checks that the processor is on the machine and that the package matches before the package is installed.
- 8.     Finish – Click Finish to upload the files and assemble the package. When the assembly process ends the button changes from Finish to Done. Click Done to
- 10    complete the package creation function.

## Define a Group / Modify a Group

This module lets an administrator group machines together, making the rollout procedures easier so that a rollout is as easy for one machine as it is for 500 machines. Additionally,

15    an administrator might group machines according to their function or location to make bandwidth utilization more efficient for their network.

1. Group Name – The label designation for the group.
2. Machine List – Select all the machines this group will include. A machine shows
- 20    up only after the update agent is installed and registered.
3. Finish – After the machines are placed in the group, the Finish button changes to Done. Click Done to complete the group function.

## Schedule a Rollout / View Existing Rollouts

25    The rollout schedule defines the date and time the packages are made available to the designated machines.

1. Choose a Package
  - Package Selection List – Choose a package (only one at this time) to install.
- 30    2. Choose Machines
  - Add a Group – This button displays a dialog box showing a list of the available groups. Highlight the groups you wish to deploy then click the OK button.
  - Remove a Group – Highlight the groups you do not want the package rolled out to, then click the Remove a Group button.
  - 35    • Add a Machine – This button displays a dialog box showing a list of available machines (with registered update agents on them). Highlight the machines to add then click the OK button.
  - Remove a Machine – Highlight the machines you do not want the package rolled out to, then click the Remove a Machine button.
  - 40    • Rollback – Removes the package just installed and returns the backup (if one was designated). This option is available only via View Existing Rollouts.
  - Reapply – Re-installs the package.
3. Choose a Rollout Date and Time
  - Calendar – Choose the date for the rollout installation to occur.
  - 45    • Time – The time on the server when the package is to be rolled out.
4. Choose Bandwidth and Sequencing

- Bandwidth – This level determines how much bandwidth on the server downloading of the package will utilize. The minimum value is 30 % and the maximum is 100%.
  - Sequencing – Selecting YES (default value) causes the rollout to go machine by machine throughout the entire rollout process and finish after the last machine is done. If an error occurs anywhere in the rollout process the rollout stops. Selecting NO causes the rollout to install the package on all machines. If an error occurs on one machine, it does not affect the package rollout on another machine.
- 5                    5. Finish – The rollout is created or updated and is saved after clicking the Done button.

Agent requests will be in the form of HTML Forms using the POST method. Host responses will be well-formed XML 1.0 documents. Most of the returned documents are of such simple structure, a DTD, Namespace, or Schema will not be included, but they will be syntactically and structurally in compliance with the XML specification. All dates and times are normalized to Coordinated Universal Time (GMT).

This describes the transaction or data flow between the Agent, the requestor, and the Host, the Update Service. All Update transactions will be initiated by the Agent, except for the case where the Host will open, send the agent ID and then close an agreed upon port and protocol at the Agent's IP address to effectively 'Ping' or notify the Agent that it should request a list of work from the host regardless of its request schedule.

#### 25    **First Contact:**

Any Agent needing to converse with the update server 528 service, will always make a request to the designated master site for the /update subdirectory. This subdirectory will be configured to return a '302 Object Moved' and its 'new' location.

As demonstrated in the following example, the agent performs a 'HEAD' request on the /update subdirectory of the www.patchlink.com site.

#### 35    **Head Request:**

HEAD /update http/1.1

The Host responds that the object is moved, and the new location can be found at the address provided by the Location: header

#### 40    **InstallShield Agent Registration:**

During the physical installation of the 'update agent', the Administrator will be required to enter some information before the agent is installed. The Admin will be required to enter the Host Name or IP Address, the Account Identifier, a GUID (Globally Unique Identifier), and the User Name and Password that was specified when registering. This data will be sent to the host to validate the ability to install the agent software, and to generate an ID for the agent.

## Agent TaskList

Once InstallShield has successfully installed the BootStrap Agent software on the computer, it's time for the agent to start working. After the agent resolves the update server 528 host site address, it posts a 'TaskList' request. A 'TaskList' is a simple list of 'Task' items the Admin has scheduled for the Agent to perform.

The BootStrap Agent must be able to:

1. Request the initial TaskList.
2. Receive the initial TaskList.
3. Understand the initial TaskList.
4. Download the Full Agent's install file.
5. Run the Agent Install.
6. Report any install problems, if so, continue as instructed
7. Start the full Agent.
8. Poll for new TaskLists
9. Understand SoftPkg IDs and dependencies and download them.
10. Initial "Action Scripts" either by invoking an external Script Engine or by invoking the Script Engine from within the Agent.

The Agent making the initial TaskList request and processing the returned response accomplishes this. For example:

### TaskList Request

POST *server\_object\_returned\_in\_firstcontact* http/1.1  
 Content-Type: text/html  
 Content-Length: 32

Action=TaskList  
 &AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50  
 &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3  
 &AgentVer=0.0  
 &LocalTime=20000628010100  
 &Status=0

In this request, the Agent's Version is 0.0. This indicates to the host that this is a new installation of the agent and that the host should prepare a 'Task' for the agent that downloads the latest versions of the appropriate agent software. In the following response, this is shown as the first 'Task' - TaskID="C1D50120-FF13-11d3-95B5-000629526438".

Whenever there has been a change to the Agent's policy, the host will include the policy data in the 'TaskList' - since this is the initial request from the agent, the policy data is included in this response.

**LocalTime** is just that the Local time (NOT GMT). This allows the server to know exactly what time it is on the Agent machine. Format is in YYYYMMDDHHMMSS.

Status tells the tasklist processor to just return a simple yes or no status if there are tasks to be done.

- 5 Status=0 means to return a normal task list. Status=1 means tell the agent if you have tasks to be done. This allows the agent to come in non-SSL and do a quick check.

### Agent Soft Package Request

- 10 The first task indicates there is a module to be installed. As shown below, the agent requests the detailed installation information from the host:

### Soft Package Request

- 15 POST *server\_object\_returned\_in\_firstcontact* http/1.1  
 Content-Type: text/html  
 Content-Length: nnnn
- Action= SOFTPKG
- 20 &AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50  
 &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3  
 &AgentVer=0.0  
 &TaskID=C1D50120-FF13-11d3-95B5-000629526438  
 &PkgID=12340000-1111-0000-0000-000000000000
- 25 &LocalTime=20000628010100

- Note that in this instance, the Agent's version is 0.0. This indicates to the host that the package to update the Agent software should be included in the TaskList response. This allows the host to dynamically determine when there is a newer version of the agent software that is available and directs the agent to update itself.
- 30

The host puts together an "Open Software Distribution" document that details the information the agent will need to be able to complete the task:

- 35 LocalTime is just that the Local time (NOT GMT). This allows the server to know exactly what time it is on the Agent machine. Format is in YYYYMMDDHHMMSS.

### Soft Package (All elements)

- 40 A soft package showing all the possible XML components (shows backup).

- ```
<?xml version="1.0"?>
<!DOCTYPE SOFTPKG SYSTEM "http://msdn.microsoft.com/standards/osd/osd.dtd">
<SOFTPKG xmlns:GX="http://www.patchlink.com/standards/osd/update.dtd"
45   GX:TaskID="C1D50120-FF13-11d3-95B5-000629526438"
   GX:PkgID="12340000-1111-0000-0000-000000000000"
   Name="12340000-1111-0000-0000-000000000000"
```

```

    GX:ReInstall="N" GX:RollBack="N">
<TITLE>Windows NT update agent</TITLE>
<IMPLEMENTATION>
  <OS VALUE="win2k"/>
5   <OS VALUE="win98"/>
  <DISKSIZE Value="123456"/>
  <CODEBASE>
    <GX:DIR ModuleID="00000104-0000-0000-0000-000000000000">
      <GX:Destination>
10     <GX:URI DateTime="20000415010100">
        <GX:URL>FILE://%TEMP%/</GX:URL>
        <GX:ACL Attrib="RWXHSMA Name="$OTHER"/>
        <GX:ACL Attrib="RWXHSMA" Group="$GROUP"/>
        <GX:ACL Attrib="RWXHSMA" Name="$USER"/>
15     </GX:URI>
      </GX:Destination>
    </GX:DIR >
    <GX:FILE Expand="N" Overwrite="Y" ModuleID="00000100-0000-0000-0000-
20 000000000000">

```

#### Soft Package Status – Success

The return codes RC and SoftPkgRC are in decimal format. SoftPkgRC denotes the overall completion of the package. Some modules could have been successful (RC=0) but another may have caused the error. If a rollout is attempted with a package that has already  
 25 been install once then the agent will return (RC=0) for all the modules it installed and return (SoftPkgRC=725003) or 0x000b100b Soft Package already installed.

Upon completion of the task, the agent will update the host with the results:

```

Request
30 POST server_object_returned_in_firstcontact http/1.1
Content-Type: text/html
Content-Length: nnn

Action=Status
35 &AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
  &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
  &AgentVer=2.0
  &TaskID=C1D50120-FF13-11d3-95B5-000629526438
  &PKGID=12340000-1111-0000-0000-000000000000
40 &InstallDate=20000101123456
  &SoftPkgRC=0
  &SoftPkgRCMsg=Success
  &ModuleID=00000100-0000-0000-0000-000000000000
  &RC=0
45 &RCMsg=Success

```

## File Attributes and ACL's

This part describes the GX:ACL element found in GX:Destination (GX:URI) element. The attributes in Update are supplied in to the agent in the Super set form defined below.

The problem with doing basic file attributes is that some file systems blur the boundary between Attributes and ACL's. An attribute is the basic ACL of a file and what is defined here is a small cross platform superset. For instance, Windows NTFS has the Read Only attribute flag but it also has the Read ACL. Therefore, if we are going to make generic attribute flags, then we must expect the meaning to be altered somewhat when used as ACL's. Those on the Unix platform will see no difference, except that like other platforms, you would ignore flags that you do not understand or no defined behavior is listed here.

Three default ACL's are defined and act like basic file attributes; \$OTHER, \$GROUP, \$USER.

On Unix the file system all three of these attribute ACL's would use. However, NT, FAT and NetWare would use only \$OTHER for basic file attributes. Any other names in the ACL's element data will be construed as a name

ACL and Attribute flags

| Letter | Short   | Definition                                                                                                        |
|--------|---------|-------------------------------------------------------------------------------------------------------------------|
| R      | Read    | Display the file's data, attributes, owner, and permissions                                                       |
| W      | Write   | Write to the file, append to the file.                                                                            |
| X      | Execute | Run the file (if it's a program or has a program associated with it for which you have the necessary permissions) |
| H      | Hidden  | Hidden file                                                                                                       |
| S      | System  | System file                                                                                                       |
| M      | Modify  | Read, write, modify, execute, and change the file's attributes.                                                   |
| A      | Archive | File is ready for Archive                                                                                         |

The XML syntax:

This denotes an ACL for a User

```
<GX:ACL Attrib="RWXHSMA" Name="UserName"/>
```

ACL for a Group. Note that \$GROUP will always use Group=

```
<GX:ACL Attrib="RWXHSMA" Group="GroupName"/>
```

**Soft Package - Rollback**

HTTP/1.1 200 OK

Connection: close

5 Content-Type: text/xml

Content-Length: nnn

```

<?xml version="1.0"?>
<!DOCTYPE SOFTPKG SYSTEM "http://msdn.microsoft.com/standards/osd/osd.dtd">
10 <SOFTPKG xmlns:GX="http://www.patchlink.com/standards/osd/update.dtd"
    GX:TaskID="C1D50120-FF13-11d3-95B5-000629526438"
    GX:PkgID="12340000-1111-0000-0000-000000000000"
    Name="12340000-1111-0000-0000-000000000000"
    GX:ReInstall="N" GX:RollBack="Y">
15 <TITLE>Windows NT update agent</TITLE>
    <IMPLEMENTATION>
        <DISKSIZE Value="432"/>
        <CODEBASE>
            <GX:FILE Expand="N" Overwrite="Y" ModuleID="00000100-0000-0000-0000-
20 000000000000">
                <GX:Destination>
                    <GX:URI>
                        <GX:URL>FILE://%TEMP%/</GX:URL>
                        <GX:FILENAME>HelloWorld.txt</GX:FILENAME>
25 </GX:URI>
                    </GX:Destination>
                    <GX:Backup>
                        <GX:URI>
                            <GX:URL>FILE://%TEMP%/Backup</GX:URL>
30 </GX:URI>
                        </GX:Backup >
                    </GX:FILE>
                </CODEBASE>
            </IMPLEMENTATION>
35 </SOFTPKG>

```

This example rolls back the simple file copy with backup shown above. The agent denotes a rollback from the attribute GX:Rollback="Y" in the SOFTPKG element tag. The GX:Source element tags are not supplied.

40 The destination MUST contain a filename to restore the backup to. (Note: it is not an error if the backup files do not exist prior to rollback (the destination may not have existed when the package was distributed). It is however, an error if the destination files exists and cannot be deleted prior to the rollback.)

45

**ProxyGet**

Sometimes an agent may be installed behind a firewall in such a configuration that the agent is only allowed access to the host site. The agent will detect this case when it tries to retrieve a module for a package that is on the vendor's site. When the agent realizes that it cannot establish communications with a standard HTTP get, it can ask the host to retrieve the file on the agent's behalf by using a 'ProxyGet' request – as described below:

#### Request

```
POST server_object_returned_in_firstcontact http/1.1
10 Content-Type: text/html
Content-Length: nnn

Action=ProxyGet
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
15 &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&URL=http://www.Microsoft.com/hotfix/Q12345.exe
```

#### 20 ProxyGetStatus

#### Request

```
POST server_object_returned_in_firstcontact http/1.1
25 Content-Type: text/html
Content-Length: nnn

Action=ProxyGetStatus
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
30 &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&RefID=107045CF06E011D28D6D00C04F8EF8E0
```

#### 35 GetRequest

```
POST server_object_returned_in_firstcontact http/1.1
Content-Type: text/html
Content-Length: nnn
40

Action=Get
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
45 &RefID=107045CF06E011D28D6D00C04F8EF8E0
```

**HTTP Get****Request:**

5 GET /download/Q12345.EXE http/1.1

**Bandwidth Utilization**10 **Range specified Get Request:**

HTTP/1.1 allows a client to request that only part (a range of) the response entity be included within the response. HTTP/1.1 uses range units in the Range and Content-Range header fields. An entity may be broken down into subranges according to various structural units.

range-unit = bytes-unit | other-range-unit

bytes-unit = "bytes"

20 other-range-unit = token

The only range unit defined by HTTP/1.1 is "bytes". HTTP/1.1 implementations may ignore ranges specified using other units. HTTP/1.1 has been designed to allow implementations of applications that do not depend on knowledge of ranges.

25 Since all HTTP entities are represented in HTTP messages as sequences of bytes, the concept of a byte range is meaningful for any HTTP entity.

Byte range specifications in HTTP apply to the sequence of bytes in the entity-body (not necessarily the same as the message-body). A byte range operation may specify a single range of bytes, or a set of ranges within a single entity.

When the administrator has selected Bandwidth Utilization features, by specifying them in the agent's policy data, the agent will make 'Range' specified Get requests rather than simple Get requests.

35

Consider the following Agent Profile:

```

40 <Policy IntervalType="S" Interval="60" Start="000000" End="060000"
    Retries="3" BackOff="10%" AlwaysUseProxyGet="Y"
    FailAction="Stop" UDPPort="1234" TCPPort="1234"
    KeepAliveConns="Y"
    DownloadRestartable="Y" DownloadChunkSize="1024"
    DownloadWaitSchedule="S" DownloadWaitInterval="10"/>
45
```

The following shows a request for the first 1024 bytes of the Q12345.Exe file, and the host's response:

**Request:**

5 GET /download/Q12345.EXE http/1.1  
Range: bytes=0-1023

**ProxyGet Request:**

10 POST *server\_object\_returned\_in\_firstcontact* http/1.1  
Content-Type: text/html  
Content-Length: nnn

Action=Get  
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50  
15 &AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3  
&AgentVer=2.0  
&RefID=107045CF06E011D28D6D00C04F8EF8E0  
&RangeBytes=0-1023

20

**Response XML Elements**

| Element | POLICY |
|---------|--------|
|---------|--------|

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attributes | <p><b>IntervalType</b> – type of time period.</p> <ul style="list-style-type: none"> <li>• S=Seconds</li> <li>• M=Minutes</li> <li>• H=Hours</li> </ul> <p><b>Interval</b> – Number of time periods that agent should check host for Tasklist.</p> <p><b>Start</b> – The time of day the agent should start running and checking for work to do (GMT).</p> <p><b>Stop</b> – The time of day the agent should stop running and checking for work to do (GMT).</p> <p><b>Retries</b> – The number of times to retry a request before applying the Backoff amount.</p> <p><b>BackOff</b> – the amount of IntervalType time to added to the Interval after a failed contact with the host. This may be expressed as a percentage by appending the percent sign (%). <b>UDPPort</b>– {nnn} UDP port number used to wake up the Agent.</p> <p><b>TCPPort</b>– {nnn} TCP port number used to wake up the Agent.</p> <p><b>TraceLevel</b> – OFF = 0, INFO = 1, DETAILED = 2, DEBUG = 3</p> <p><b>PurgeIntervalType</b> – type of time period (see IntervalType)</p> <p><b>PurgeInterval</b> – Number of time periods (PurgeIntervalType) that the agent should scan backups and purge those with a time older than the purge interval.</p> |
| Child of   | TASKLIST                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Parent of  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| Element    | TASK                                                                                                          |
| Attributes | <p><b>TaskID</b> – unique task identifier.</p> <p><b>PkgID</b> – The package identifier to be acted upon.</p> |
| Child of   | TASTLISK                                                                                                      |
| Parent of  |                                                                                                               |

## 5 Discovery Agent XML tags

<name> tag - This is the name of the file you want to search for.

- <path> tag - Very versatile. This is the path you want to search for the file in.

<Version> tag - This is the version of the file you are looking for.

<created> tag - This is the date the file was created.

Example <version> > 5/30/2001 12:01:04 PM </version>

5 Note: This exact date format is preferred.

<Size> tag - This is the size of the file you are looking for. Note: Cannot due < or >

<root> tag - This is the root key to look for the registry entry in.

10

<Key> tag - This is the key in the registry you are looking for.

<value> tag - this is the value in the key you are looking for.

15 <Data> tag - this is the data you expecting to find in that key.

<class> tag - You can specify any valid WMI class that makes sense. example  
win32\_services

20 <searchfield> - This is the field that will best determine what wmi entries to look at.

<searchvalue> - This is the value that will best determine what wmi entries to look at.

<checkfield> - This is the field to look in to get the value you are expecting to get.

25

<checkvalue> - This is the value you are expecting to find.

Example of the <registry> section of the input file.

30

```
<registry componentid="" reportID="">
```

```
<root> </root>
```

```
<key> </key>
```

```
<value> </value>
```

35

```
<data> </data>
```

```
</registry>
```

### Patch Fingerprint Signature example

```
<report reportid="22">
```

40

```
<file componentid="1" reportID="1">
```

```
<name>outlook.exe</name>
```

```
<path></path>
```

```
<version></version>
```

```
<created></created>
```

45

```
<size>57393</size>
```

```
<root>HKEY_LOCAL_MACHINE</root>
```

```
        <Key>SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\OUTLOOK.EXE</key>
        <value>Path</value>
    </file>
5  </report>
```

The Above example will find the outlook Path from the registry and then will validate its size.

10

## Summary

The invention provides systems, methods, and configured storage media for assuring that software updates are needed, and that the computers have the necessary software and hardware components, then updating the software across a network with little  
15 or no need for human oversight, without requiring copies of the software patches on an administrative machine on the network whose clients are being updated, and which removes the updates from the affected machines, leaving them in a usable state when a problem is discovered during installation or after installation with an installed patch.

As used herein, terms such as “a” and “the” and item designations such as “update  
20 server” are inclusive of one or more of the indicated item. In particular, in the claims a reference to an item means at least one such item is required. When exactly one item is intended, this document will state that requirement expressly.

The invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects  
25 only as illustrative and not restrictive. Headings are for convenience only. The claims are part of the specification which describes the invention. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

30 What is claimed and desired to be secured by patent is:

## CLAIMS

1. An automated method for at least attempting to update software in a system having a first target computer in a non-update state connected across a network to an update server in a pre-update state, the system also having a package computer which is  
5 inaccessible to the first target computer but accessible to the update server, and a repository component accessible to the first target computer and the update server, the method comprising the steps of:
  - putting at least one patch fingerprint which defines a specific software update into the repository component, the patch fingerprint comprising a patch  
10 signature and an existence test;
  - gathering information about the first target computer and sending the information back to the repository component;
  - comparing at least a portion of the gathered information with the patch fingerprint to determine if the specific software update is absent from the target  
15 computer;
  - if a known condition is met, then placing at least one task identifier on an update task list, the task identifier specifying the first target computer, the update task list stored at the update server, the task identifier also specifying at least one  
20 download address which references a location on the package computer that contains a software update for the first target computer;
  - starting a task in response to the task identifier, the task attempting a first download of the software update from the package computer to the update server;
  - if the first download completes successfully, then attempting a second download of the software update from the update server to the first target  
25 computer; and
  - monitoring the attempted downloads for an outcome.
2. The method of claim 1, wherein the known condition is the software update being absent from the target computer.
3. The method of claim 1, wherein information about the target computer  
30 comprises at least one of: hardware configuration, current software installed, specific

software updates installed, registry information, file information, services currently running, web information, and configuration information.

4. The method of claim 1, further comprising a patch locating step which monitors at least one patch component database location for a new patch fingerprint, and  
5 wherein the putting step further comprises downloading the new patch fingerprint into the repository component after the new patch is located.

5. The method of claim 1, wherein the system further comprises a patch component database which signals the repository component that a new patch fingerprint is available, and wherein the putting step further comprises downloading the new patch  
10 fingerprint into the repository component after the new patch is located.

6. The method of claim 1, wherein the patch signature consists of specific computer information, the method further comprises the step of the repository component sending the patch signature to the target computer, and the gathering step further comprises the target computer gathering the specific computer information mentioned in  
15 the patch signature, and then sending the gathered computer information back to the repository component.

7. The method of claim 1, wherein the comparing step further comprises using the existence test together with the at least a portion of the gathered information to determine if the specific software update is absent from the target computer.

20 8. The method of claim 1, wherein the patch fingerprint further comprises patch inventory information, the system includes an inventory database containing target computer information and wherein the gathering step is started only if the target computer information and the patch inventory information match.

9. The method of claim 1, wherein the method further comprises notifying an  
25 administrator after the comparing step wherein notifying an administrator comprises sending a message to a predetermined address at least one of: an email message, a pager message, an instant message, a SNMP notification, and a voice mail message.

10. The method of claim 9, wherein the system comprises at least two target computers and the message comprises a list of all target computers from which the  
30 software update is absent and wherein the known condition to be met prior to placing the

task identifier on the update task list is a message from the administrator indicating consent.

11. The method of claim 1, wherein the method further comprises suspending the task after the monitoring step detects a download failure and then restoring the first  
5 target computer to the non-update state.

12. The method of claim 1, which further comprises removing the software update from the first target computer after the monitoring step detects a failure.

13. The method of claim 1, wherein the system includes at least two target computers both of which have received the download of the software update and wherein  
10 the monitoring step records an outcome of failure on at least one of the updated computers, further comprising the step of removing the updates from the at least two updated target computers.

14. The method of claim 1, wherein there are at least two package computers and the offsite update server determines which package computer to download the  
15 software update from based on a predetermined criterion.

15. The method of claim 1, wherein between the first and second downloads the method includes a delay step wherein the second download is delayed for a period which is based on a predetermined criterion.

16. The method of claim 15, wherein the delay step specifies a time delay and  
20 the specified time delay is based on an estimate of the time needed to download the software update from the package computer to the update server.

17. The method of claim 1, wherein there is at least a second target computer, the offsite update server contains an offsite update server list that lists each target computer that is to receive the software update, and the method further comprises the step  
25 of checking the offsite update server list for a target computer that has not received the update and if one is found, adding an update task identifier for that target computer to the update task list.

18. The method of claim 17, wherein the checking step is performed after the monitoring step determines that the outcome is successful.

19. The method of claim 1, wherein an outcome of success in the monitoring  
30 step is indicated by the target computer sending a message to the update server after the

second download has completed successfully, and wherein an outcome of failure in the monitoring step is indicated by the update server not receiving a message from the target computer within a time period that is based on a predetermined condition.

20. The method of claim 1, wherein the monitoring step further comprises  
5 watching the first target computer, for a time period that is based on a predetermined criterion, to at least attempt to detect abnormal activity associated with running the software update, and if abnormal activity is detected during the time period then declaring the outcome of the monitoring step to be failure.

21. The method of claim 1, wherein the monitoring step further comprises  
10 accepting messages from a help desk service, for a time period that is based on a predetermined criterion, to at least attempt to detect abnormal activity associated with running the software update, and if abnormal activity is reported during the time period then declaring the outcome of the monitoring step to be failure.

22. The method of claim 1, wherein the monitoring step further comprises  
15 notifying an administrator of the outcome, wherein notifying an administrator comprises sending to a predetermined address at least one of: an email message, a pager message, an instant message, a fax, a SNMP notification, or a voice mail message.

23. A target computer in a non-updated state which is located in a network and which is configured to attempt to receive a software package across the network, and to  
20 attempt to install on itself a received software package to update software, at least one update server being accessible to the network through a remote connection, a target computer update list on the update server containing a reference to a software package location; the target computer comprising:

memory;  
25 a network connection;  
an update agent that reads the target computer update list from the update server, uses the reference to the software package to locate the software package;  
an installer that attempts to install the software package on the target computer;  
30 an outcome finder that determines if the software package installation was successful; and

a restorer that restores the target computer to a non-updated state if the outcome finder determines that the software package installation was not successful.

24. The target computer of claim 21, in combination with the update server to  
5 form a system.

25. The system of claim 24, wherein the update list further comprises a date, and wherein the update agent will wait at least until the date before attempting to download the software package.

26. The target computer of claim 24, wherein there are at least two update  
10 servers and the update agent determines which update server to utilize using at least one predetermined criterion.

27. The target computer of claim 26, wherein the predetermined criteria includes at least one of: selecting the first update server that is available, and selecting the least-busy update server.

28. The target computer of claim 23, wherein the target computer cannot  
15 directly access the software package, the update server can directly access the software package, and wherein the installer first attempts to download the software package to the update server memory, and if the first download is successful, the installer then attempts to download the software package from the update server memory to the target computer  
20 memory.

29. The target computer of claim 28, wherein the software package is kept in the update server memory and then deleted from the update server memory after at least one predetermined criterion is met.

30. The target computer of claim 28, wherein the update agent residing on the  
25 target computer initially checks the update server for the software package in the update server memory and if the software package is found there, the target computer downloads the software package directly from the update server.

31. The target computer of claim 23, wherein the software package is owned by an update host and is leased from the update host by a user.

32. The target computer of claim 23 in combination with the update server,  
30 wherein the update server is accessible to the target computer through a firewall and

wherein the update server must provide authentication before it can be accessed by the target computer.

33. The target computer of claim 23, further comprising means for notifying an administrator of the outcome finder results wherein the means for notifying comprises at least one of: email messages, pager messages, instant messages, SNMP notification, and voice mail messages.

34. The target computer of claim 23, wherein the location of the software package is specified by at least one of: a Uniform Resource Locator and a fully qualified domain name.

35. The target computer of claim 23, wherein the software package includes at least one of: a software patch to an existing file, at least one file to install a software application that has not previously been installed on the target computer, a data file, a script file, an executable file, and an update of the update agent.

36. The target computer of claim 23, in combination with a repository component which stores information about the target computer, the target computer further comprising a discovery agent that gathers information about the target computer and reports that information back to an inventory library in the repository component.

37. The target computer of claim 36, wherein the information gathered comprises at least one of: usage statistics, hardware configurations, current software installed, specific updates installed, specific patches installed, registry information, file information, services currently running, patch signatures utilized, and configuration information.

38. The target computer and repository component system of claim 36, further comprising at least one patch fingerprint which contains information used to determine whether a software package associated with the patch fingerprint is installed on the target computer, the patch fingerprint comprising a patch signature and an existence test.

39. The system of claim 38, the patch fingerprint further comprising general install information and the system including an evaluator which evaluates at least a portion of the stored inventory library information about the target computer using the general install information to determine if the software package associated with the patch fingerprint can be installed on the target computer.

40. The system of claim 39, wherein the patch signature includes a request for specific install information, the discovery agent first locates in the target computer the specific install information, mentioned by the patch signature, and then sends the specific install information back to the repository component.

5        41. The system of claim 40, wherein the evaluator uses the existence test and the specific install information to determine if the software package associated with the patch fingerprint is installed on the target machine.

42. The system of claim 39, wherein the evaluator determines if the target computer possesses a necessary computer configuration to successfully install the software package associated with the patch fingerprint.

43. The system of claim 42, wherein the necessary computer configuration comprises at least one of: a software package that should be present, a hardware component that should be present, a software package that should be removed, a hardware component that should be removed.

15        44. The system of claim 39, further comprising a patch component database which includes new patch fingerprints, and wherein a downloader is signaled when a new patch fingerprint is installed on the patch component database.

45. The system of claim 44, wherein there are at least two target computers, the system further comprising a separate target inventory for each of the at least two target computers, wherein a notifier uses the evaluator in combination with the target inventories to create the update list which identifies zero or more target computers wherein the software package associated with the patch fingerprint is absent, and the notifier then notifies at least one administrator of the update list.

25        46. The system of claim 45, further comprising a report generator which generates reports comprising a list of zero or more computers wherein the patch is absent as well as a list of zero or more computers wherein the patch is present.

47. The system of claim 45, wherein notifying an administrator comprises sending at least one of an email, pager, telephone message, instant message, fax, beeper, or SNMP notification to a predetermined address.

30        48. The system of claim 45, wherein the patch component database is owned by an update host, the target computer has an owner, and the downloader is allowed to

replicate the new patch fingerprint and associated patch information only if the target computer owner has permission from the update host.

49. The system of claim 48, wherein the permission consists of at least one of: a purchase agreement, a lease agreement, an evaluation agreement.

5 50. The target computer of claim 23 in combination with the update server, wherein the target computer further comprises a current configuration, and the update server further comprises a recommended configuration, the system further comprising a surveyor which scans the target computer for its current configuration, compares the current configuration to the recommended configuration, and then prepares a proposed  
10 update list utilizing the current configuration and the recommended configuration.

51. The system of claim 50, wherein a new target computer is added to the system, the surveyor scans the new target computer generating an update list, and an administrator is automatically notified of the update list for the new target computer.

52. The system of claim 51, wherein the new target computer usage is restricted  
15 until a predetermined condition is met.

53. The system of claim 52, wherein the predetermined condition comprises at least one of: the new target computer is updated to at least partially meet the update list, the administrator gives permission.

54. The target computer of claim 23 in combination with the update server,  
20 wherein the update server further comprises a backup creator, and wherein the backup creator creates a copy of the target computer before the installer installs the software package, and wherein the copy of the target computer is used by the restorer to restore the target computer to the non-updated state if the outcome finder determines that the software package installation was not successful.

25 55. The system of claim 53, wherein the copy of the target computer is stored in a memory of the update server.

56. A configured program storage medium having a configuration that represents data and instructions which will cause at least a portion of a computer system to perform method steps for at least attempting to update software in a system having a first  
30 target computer in a pre-update state connected across a network to an update server in a pre-update state, the system also having a package computer which is inaccessible to the

first target computer but accessible to the update server, and a repository component accessible to the first target computer and the update server, the method comprising the steps of: gathering information about the first target computer and sending the information back to the repository component; putting at least one patch fingerprint which defines a specific software update into a repository component, the patch fingerprint comprising a patch signature and an existence test; comparing at least a portion of the gathered information with the patch fingerprint using the existence test to determine if the specific software update is absent from the target computer; if a known condition is met then placing at least one task identifier on an update task list, the task identifier specifying the first target computer, the update task list stored at the update server, the task identifier also specifying at least one download address which references a location on the package computer that contains a software update for the first target computer; starting a task in response to the task identifier, the task attempting a first download of the software update from the package computer to the update server; if the first download completes successfully, then attempting a second download of the software update from the update server to the first target computer; and monitoring the attempted downloads for an outcome.

57. The configured storage medium of claim 56, wherein the known condition is the software update being absent from the target computer.

58. The configured storage medium of claim 56, wherein information about the target computer comprises at least one of: hardware configuration, current software installed, specific software updates installed, registry information, file information, services currently running, and configuration information.

59. The configured storage medium of claim 56, wherein gathered information is placed in a database in the repository component such that the information about the target computer can be accessed by the repository component.

60. The configured storage medium of claim 56, further comprising a patch locating step which monitors at least one patch component database location for a new patch fingerprint, and wherein the putting step further comprises downloading the new patch fingerprint into the repository component after the new patch is located.

61. The configured storage medium of claim 56, wherein the method further comprises notifying an administrator after the comparing step wherein notifying an administrator comprises sending a message to a predetermined address at least one of: an email message, a pager message, an instant message, a SNMP notification, or a voice mail  
5 message.

62. The configured storage medium of claim 61, wherein the system comprises at least two target computers and the notifying an administrator message comprises a list of all target computers that lack the software update.

1/8

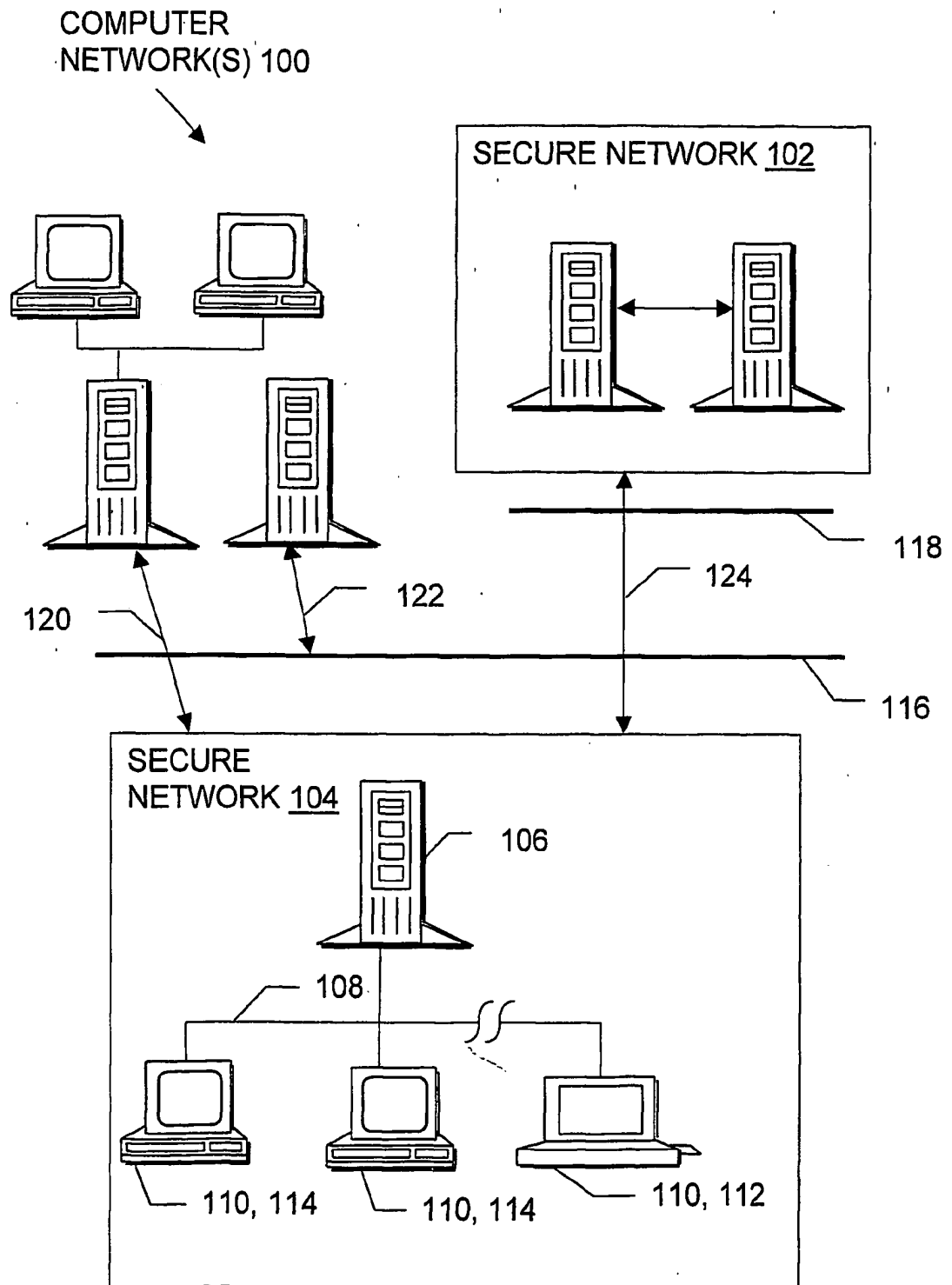


Fig. 1

2/8

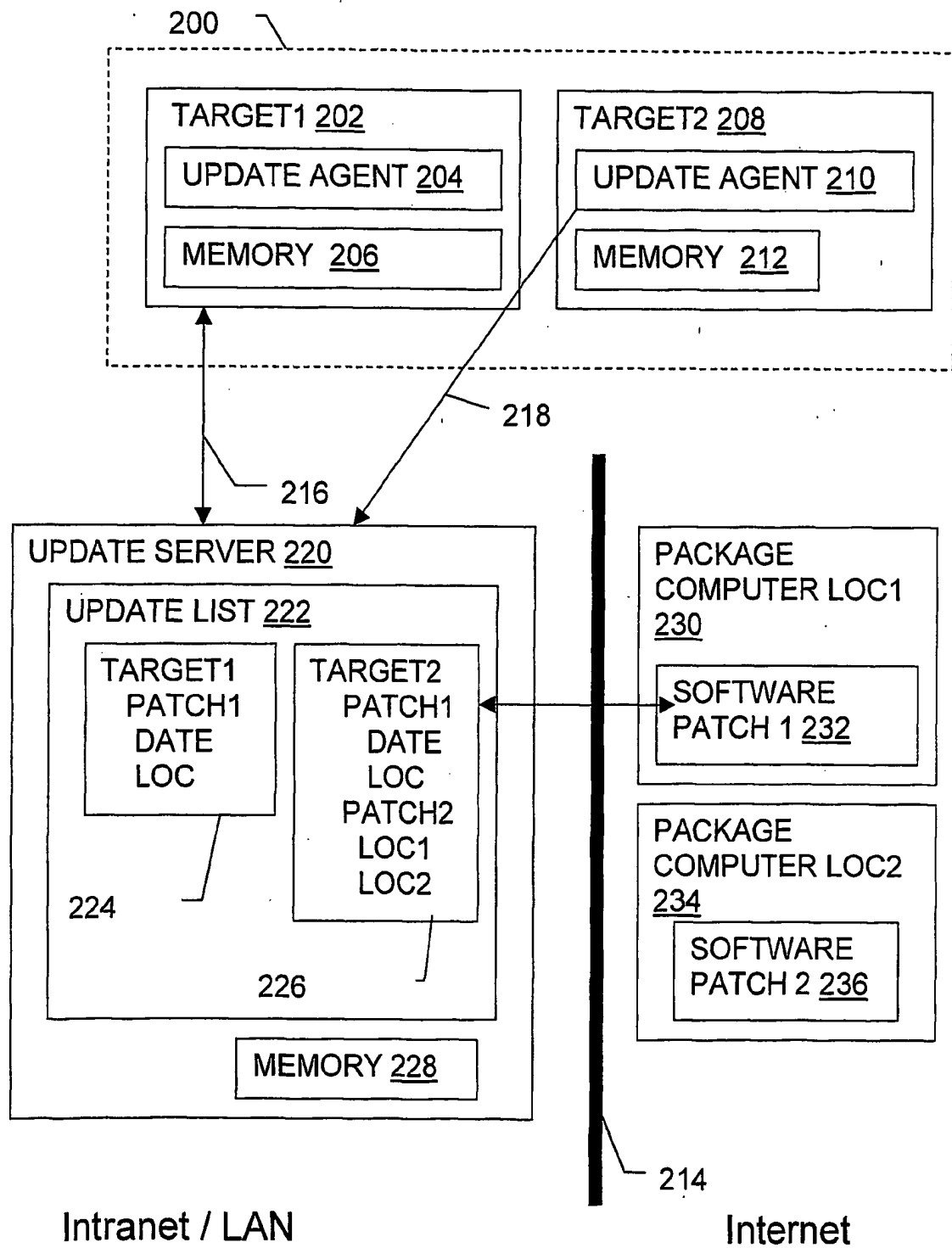


Fig. 2

3/8

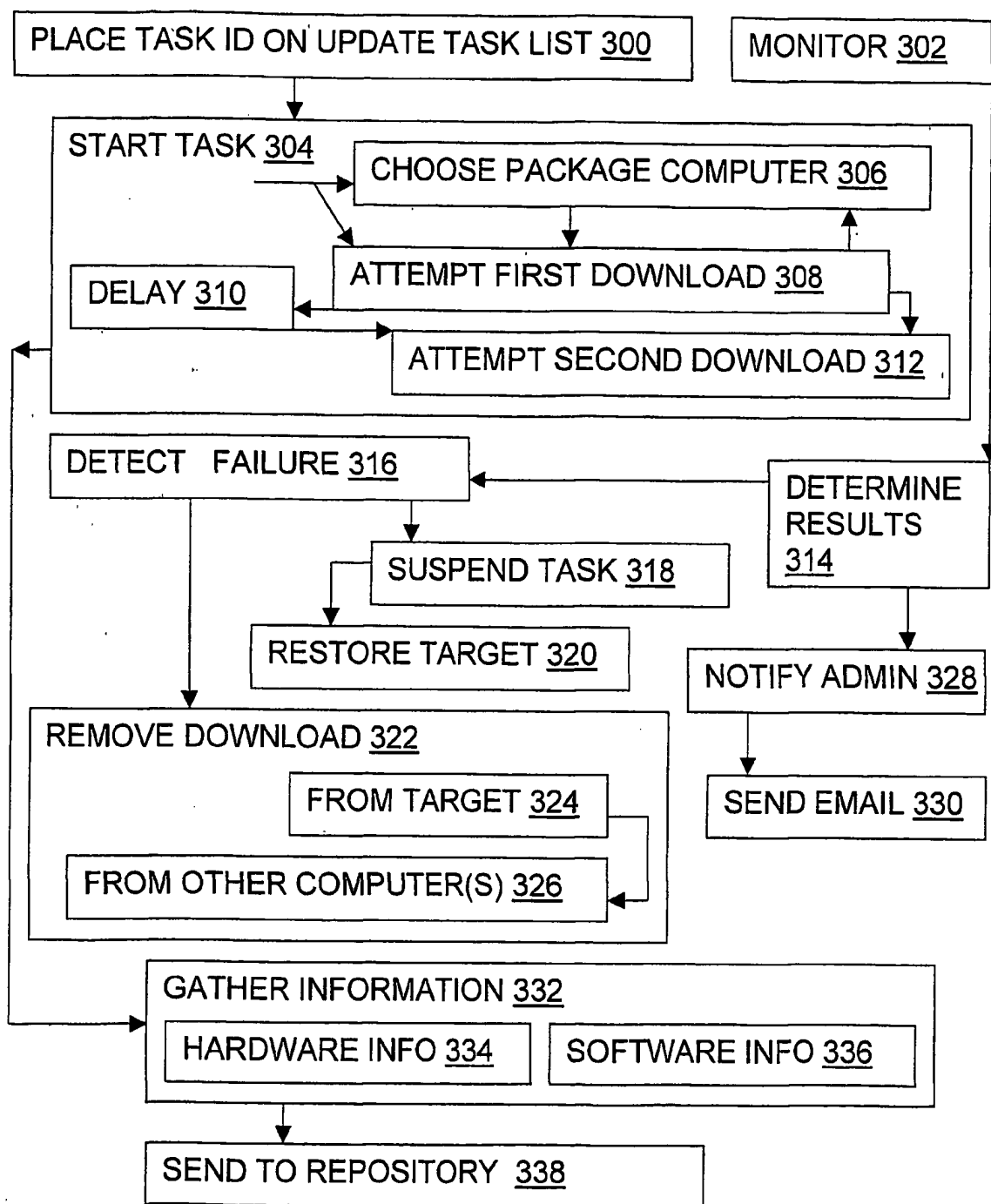


Fig. 3

4/8

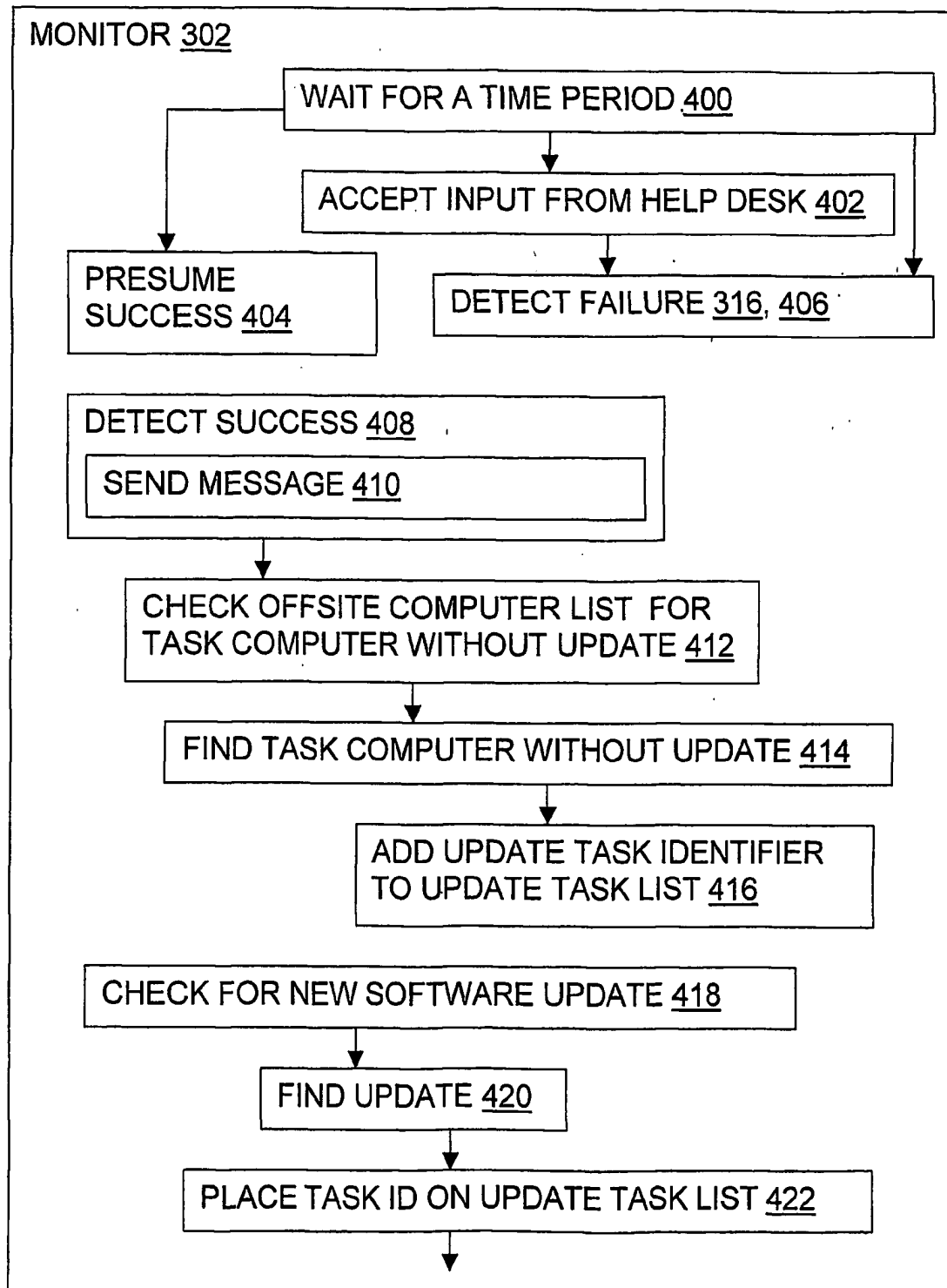


Fig. 4

5/8

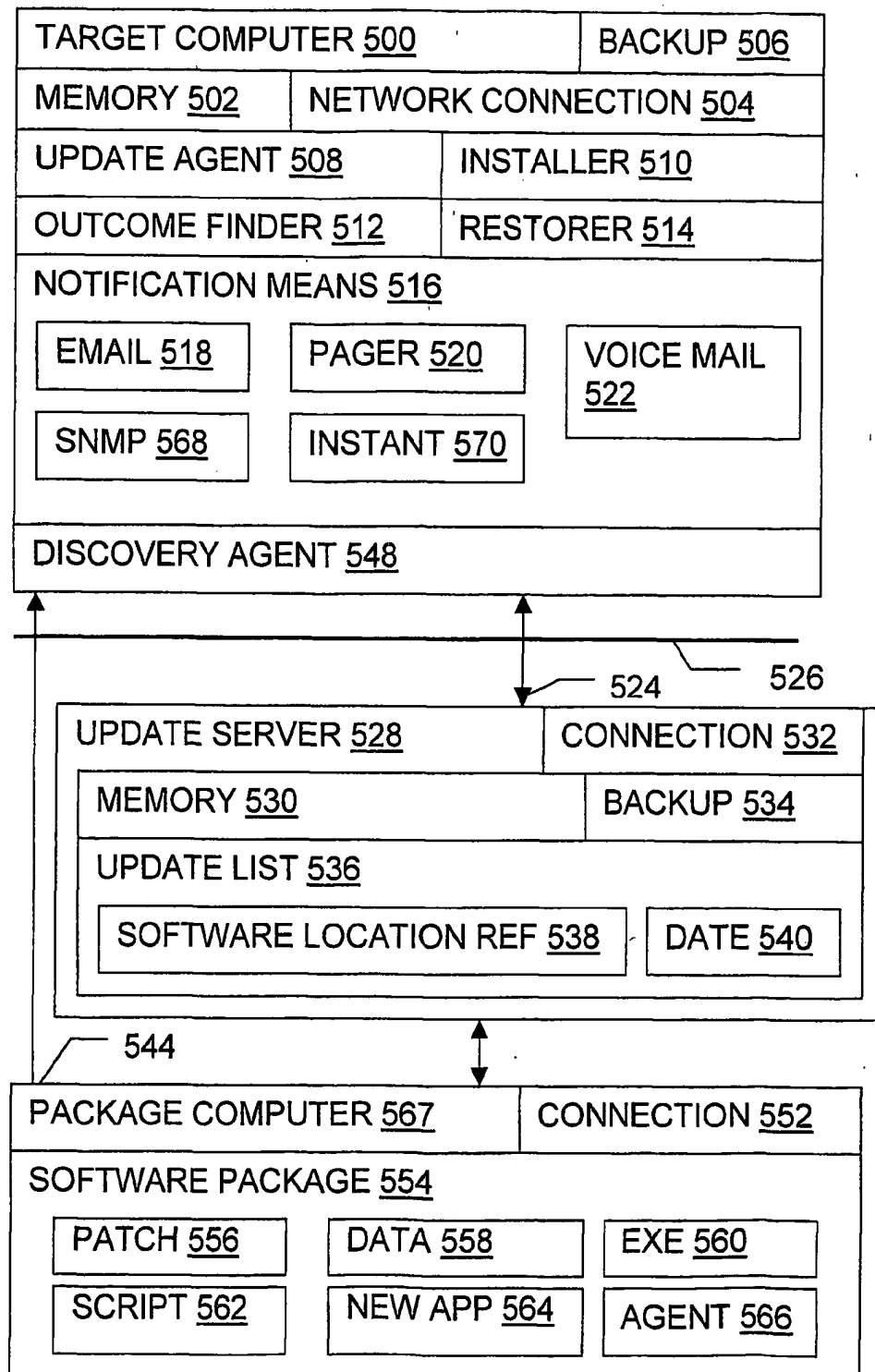


Fig. 5

6/8

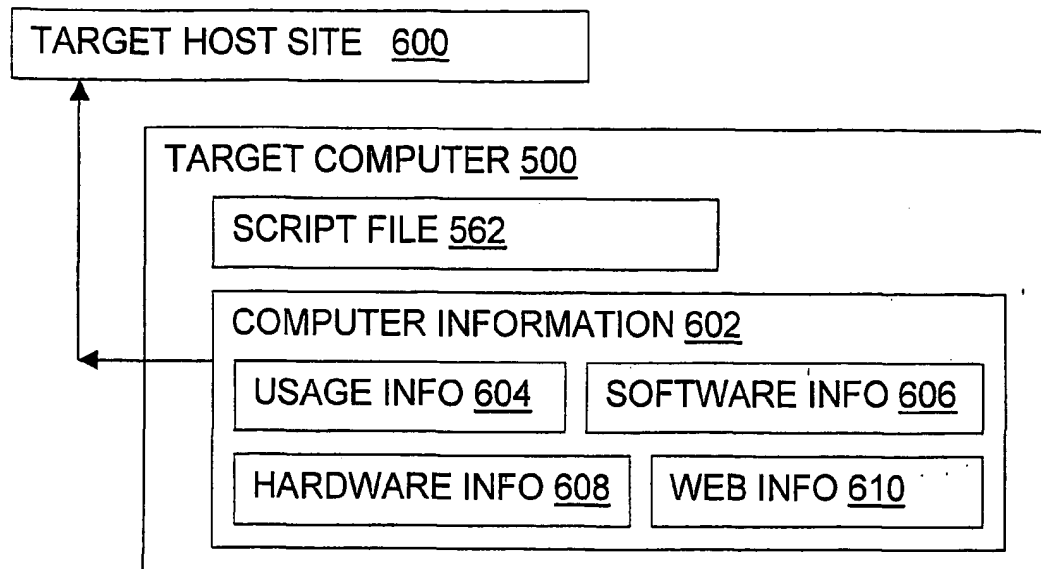


Fig. 6

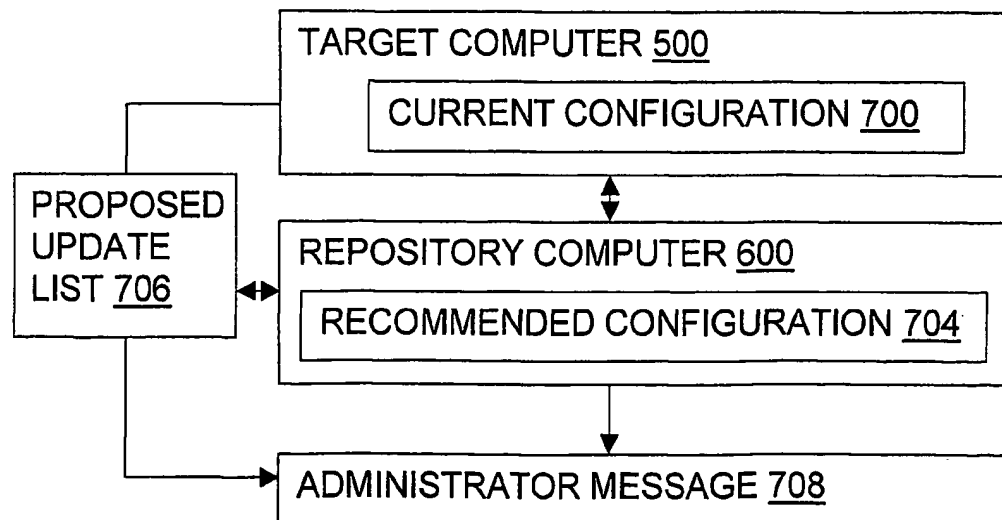


Fig. 7

7/8

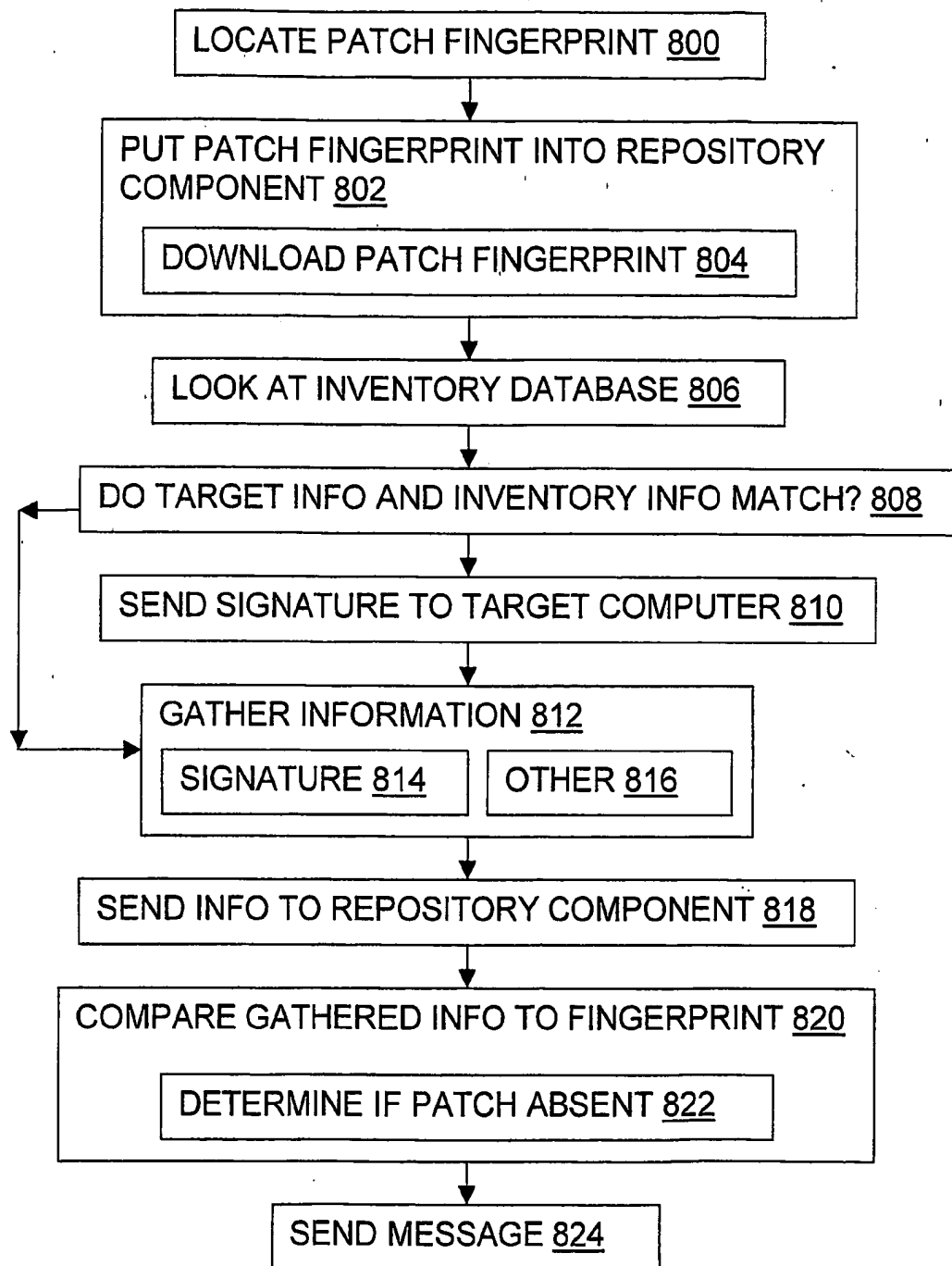


Fig. 8

8/8

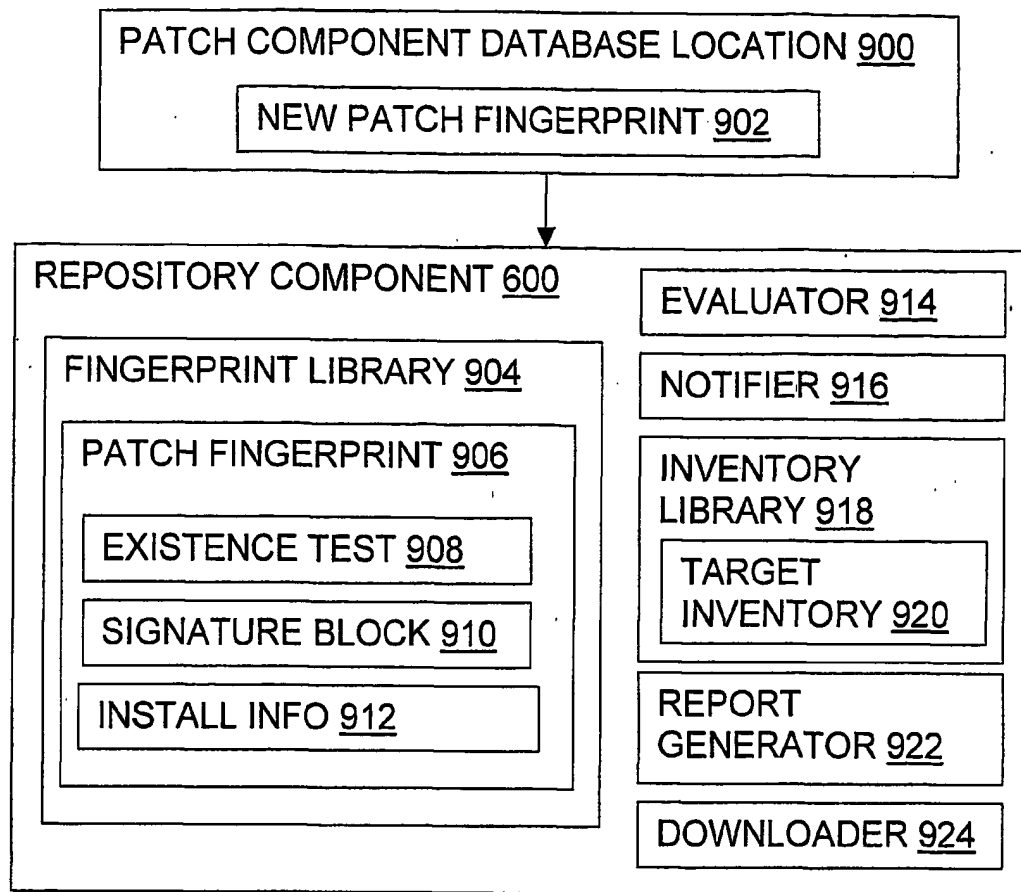


Fig. 9

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/29863

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7) : G06F 9/455

US CL : 717/1, 717/11, 707/203, 707/204

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 717/1, 717/11, 707/203, 707/204

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
ACM, IEEEElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
EAST, WEST**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,860,012 A [LUU] 12 JANUARY 1999, col 1-2, lines 60-67 and lines 1-17	1-62
Y	US 5,649,187 A [HORNBUCKE] 15 JULY 1997, col 1-4, lines 19-67, lines 1-67	1-62

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 06 DECEMBER 2001	Date of mailing of the international search report 02 JAN 2002
-------------------------------------------------------------------------------	-------------------------------------------------------------------

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

ANIL KHATRI

Telephone No. (703) 305-3703